Prosecuting Intellectual Property Crimes

Fourth Edition

H. Marshall Jarrett
Director, EOUSA

Cameron G. Chandler
Director, OLE

OLE Litigation Series

Ed Hagen
Assistant Director, OLE

Andrea Sharrin
Deputy Chief for Intellectual Property
CCIPS
Criminal Division

Published by
Office of Legal Education
Executive Office for
United States Attorneys

Table of Contents

Preface and Acknowledgements

This publication is the fourth edition of the "Prosecuting Intellectual Property Crimes" Manual and provides significant updates to the comprehensive 2006 edition. It examines in depth all areas of prosecuting intellectual property crimes and incorporates a number of recent changes to the case law, statutes, and sentencing guidelines. Throughout, the material is presented in a way that is intended to provide the most practical use to prosecutors.

This publication is the result of a tremendous amount of work by many individuals in the Computer Crime and Intellectual Property Section. Kendra Ervin assumed primary responsibilities as Managing Editor as well as providing substantive updates to chapters. Many other CCIPS attorneys made significant contributions as well, including in alphabetical order: Thomas Dougherty, Scott Eltringham, Jason Gull, Eric Klumb, Brian Levine, Evan Williams and John Zacharia. Former CCIPS attorneys whose efforts also contributed include Matthew Bassiur, Mark Krotoski, Tyler Newby and Tara Swaminatha. CCIPS supervisory paralegal specialist Kathleen Baker deserves special mention for her superior editing and proofing contributions. Other paralegals and summer interns who contributed to this publication over the past few years include: Allyson Bennett, Jarrell Cook, Glenn Gordon, Lily Hines, Michael McCluskey, and John Sprangers.

Finally, we are grateful to Ed Hagen and others at the Office of Legal Education for putting this Manual into final form worthy of publication.

This Manual is intended as assistance, not authority. The research, analysis, and conclusions herein reflect current thinking on difficult areas of the law; they do not represent the official position of the Department of Justice or any other agency. This Manual has no regulatory effect, confers no rights or remedies, and does not have the force of law or a U.S. Department of Justice directive. *See United States v. Caceres*, 440 U.S. 741 (1979).

If you have questions about anything in this book, we invite you to call the Computer Crime and Intellectual Property Section at (202) 514-1026.

Attorneys are on duty every day for the specific purpose of answering such calls and providing support to U.S. Attorney's Offices nationwide.

Andrea M. Sharrin,
Deputy Chief
Computer Crime & Intellectual Property Section
Criminal Division
Department of Justice

I.
Intellectual Property—An Introduction

A. Why Is Intellectual Property Enforcement Important?

Intellectual property (IP), including creative works protected by copyright, brand identification protected by trademark, and novel inventions protected by patents and trade secret law, encompasses a vital component of the U.S. economy and, increasingly, the world's collective wealth. American music, motion pictures, business and entertainment software, as well as American brands, form an important part of America's cultural identity. The U.S. is also home to some of the world's largest manufacturers and most innovative companies, whose sought-after products are exported throughout the world. According to the Department of Commerce, in 2010 "IP-intensive industries"—those most reliant on copyright, trademark and patent protection—accounted for more than 27 million or more than one sixth of all jobs in the U.S., and more than one third of the U.S. gross domestic product. Department of Commerce, *Intellectual Property and the U.S. Economy: Industries in Focus* at vi-vii (March 2012), *available at* http://www.esa.doc.gov/sites/default/files/reports/documents/ipandtheuseconomyindustriesinfocus.pdf. Effective IP enforcement can help to preserve and create jobs and economic growth by fostering a level playing field for fair competition in the global marketplace.

Protecting IP rights is essential to fostering the innovation and creativity which fuels the U.S. economic engine. IP rights create incentives for entrepreneurs, artists, firms, and investors to commit the necessary resources to research, develop, and market new technologies and creative works. As one court observed, "[t]he future of the nation depends in no small part on the efficiency of industry, and the efficiency of industry depends in no small part on the protection of intellectual property." *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 180 (7th Cir. 1991).

The criminal enforcement of IP rights plays a critical role in safeguarding U.S. economic and national security interests as well as protecting the health and safety of consumers worldwide. The impact of today's IP crime is not limited to the economic challenges associated with piracy, counterfeiting, or trade secret theft. Inferior, unsafe counterfeits, ranging from electrical equipment to auto parts to pharmaceuticals, not only defraud ordinary consumers, but also can pose significant risks to their health and safety. The potential harm from counterfeit goods is further compounded when those goods enter the government or military supply chain, where they can impact the safety of our Armed Forces, and even compromise national security. Likewise, our national security interests can be undermined by foreign and domestic competitors who deliberately target leading U.S. industries and technologies to obtain sensitive trade secrets that have applications in defense, security, or critical infrastructure.

This is a dynamic time for IP enforcement. New technology and more sophisticated methods of manufacturing and distribution have created unprecedented opportunities for legitimate businesses, both large and small, to develop their products and market and distribute them around the world. Manufacturers and consumers are increasingly interconnected due to advances in telecommunication networks, integrated financial markets, and global advertising. Consumers enjoy near-immediate access to almost any product manufactured in the U.S. or abroad. They can provide instant payment through an international credit card system or online payment processors and receive their purchase either through immediate downloading of digital content or overnight shipment of tangible goods through express courier services. Companies and their employees also can conduct business seamlessly from anywhere in the world. Virtually all business records, research, and sensitive information exists in digital form and can be stored, accessed, copied, and transmitted using computer networks, cloud storage, and large capacity mobile devices.

Unfortunately, IP criminals exploit the benefits of these advances to support illegal piracy and counterfeiting operations. U.S. companies suffer substantial losses from international trade in counterfeit and pirated goods, which the OECD has estimated to amount to hundreds of billions of dollars each year. *See* Organization for Economic Cooperation and Development, *Magnitude of Counterfeiting and Piracy of Tangible Products: An Update* (November 2009); Frontier Economics, *Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy* (February 2011) (suggesting the value of counterfeit

and pirated products for G20 nations was $650 billion in 2008 and likely to more than double by 2015).

Although quantifying the economic effects of counterfeit and pirated goods with precision is difficult, the problem is undeniably sizable with substantial consequences: to industry in the form of lost sales, lost brand value, and reduced incentives to innovate; to consumers who use or ingest substandard or unsafe counterfeit goods; to governments which may lose tax revenue and face risks of counterfeits entering national security or critical infrastructure supply chains; and to economic growth slowed by reduced innovation and lost trade revenue. *See* U.S. Government Accountability Office, *Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods* (Publication Number GAO-10-423) (April 2010).

In addition to piracy and counterfeiting, corporate- and state-sponsored trade secret theft is on the rise and increasing in size and scope. Whether committed by corrupt insiders or foreign actors, the Internet and new technologies have enabled criminals to steal massive amounts of sensitive information almost instantaneously while remaining difficult to detect. *See* Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace, available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf. As leaders in innovation, U.S. companies are prime targets for the misappropriation of valuable and sensitive trade secrets, particularly by foreign competitors. Trade secrets may represent years of research and development to a company, with billions of dollars in related costs, and may constitute a substantial portion of the company's worth. Trade secret theft can financially devastate an individual victim and, when committed for the benefit of a foreign entity, can undermine the economic competitiveness of the U.S. as a whole. In cases involving critical technologies with military or other sensitive applications, trade secret theft can also pose a risk to national security.

Recognizing the escalating and serious threats posed by IP crime, Congress, the Administration, and the Department of Justice have all taken steps to enhance IP enforcement domestically and abroad. In the last five years, Congress has enacted several major pieces of legislation to enhance criminal enforcement tools to combat IP crime, including amendments to the statutes criminalizing trademark counterfeiting, criminal copyright infringement, and economic espionage. As of the writing of this Manual, the United States Sentencing Commission is considering amendments to the Sentencing

Guidelines applicable to offenses involving trade secret theft, counterfeit drugs, and counterfeit military goods or services.

In the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act), Pub. L. No. 110-403, § 101, 122 Stat. 4256 (2008), Congress established the Intellectual Property Enforcement Coordinator (IPEC) position to serve in the Executive Office of the President. Among other things, the IPEC brings a coordinated government-wide approach to IP enforcement. The Department worked closely with the IPEC in developing the 2010 Joint Strategic Plan on Intellectual Property Enforcement (June 2010) and the 2013 Joint Strategic Plan on Intellectual Property Enforcement (forthcoming), the IPEC's Annual Report on IP Enforcement, the Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations (March 2011), and the Administration Strategy on Mitigating the Theft of U.S. Trade Secrets (February 2013), among other efforts. *See* http://www.whitehouse.gov/omb/intellectualproperty. The Department plays a significant role in implementing the criminal enforcement aspects of the Administration's strategies.

Attorney General Holder has also made the investigation and prosecution of IP crime a top law enforcement priority. Although a well-developed civil enforcement regime in the U.S. allows IP owners to enforce their rights and obtain compensation for losses, civil enforcement alone is insufficient to address the increasingly sophisticated nature and broad scope of IP infringement. Criminal sanctions are critical to deter and hold accountable the most egregious IP violators. To this end, in February 2010, the Attorney General established a Task Force on Intellectual Property as part of a Department-wide initiative to confront the growing number of domestic and international IP crimes. The IP Task Force, chaired by the Deputy Attorney General and comprising senior Department officials from components with a stake in IP enforcement, including the Criminal Division and Executive Office of the U.S. Attorneys, has brought a coordinated approach and high-level support to the Department's overall efforts to combat IP crime. *See* http://www.justice.gov/dag/iptaskforce/.

Through the IP Task Force, the Department recommends that prosecutors prioritize IP investigations and prosecutions involving health and safety, trade secret theft and economic espionage, and large-scale criminal copyright infringement and trademark counterfeiting. Prosecutors are also encouraged to pay particular attention to those offenses committed or facilitated by use of the

Internet, perpetrated by organized criminal networks or repeat offenders, and those cases that are international in scope.

The Department pursues a three-front approach to ensure aggressive and effective prosecution. First, the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS), based in Washington, D.C., provides a core team of expert IP prosecutors who investigate, prosecute, and coordinate national multi-district and international IP cases. This group of specialists helps develop and implement the Department's overall IP enforcement strategy, and provides training and 24/7 support to Assistant U.S. Attorneys nationally. This Manual, for instance, is one of the training tools that CCIPS provides.

Second, because primary responsibility for prosecution of federal crimes generally—and IP offenses specifically—falls to the ninety-three U.S. Attorneys' Offices across the U.S. and its territories, the Department has designated at least one, and often more than one, Computer Hacking and Intellectual Property ("CHIP") Coordinator in every U.S. Attorney's Office in the country. CHIP Coordinators are Assistant U.S. Attorneys with specialized training in prosecuting IP and computer crime offenses and who serve as subject-matter experts within their districts. As of this writing, there are over 260 CHIP prosecutors designated to handle both computer crime and IP matters nationwide.

Third, CHIP Units augment the extensive network of CHIP prosecutors. Each CHIP Unit consists of a concentrated number of trained Assistant U.S. Attorneys in the same office. CHIP Units are strategically located in districts that experience a higher incidence of IP and cyber-crime, or where such crimes have the highest economic impact. These specialized squads focus on prosecuting IP offenses such as trademark counterfeiting, criminal copyright infringement, and theft of trade secrets. In addition, they prosecute high-technology offenses including computer hacking, virus and worm proliferation, Internet fraud, and other attacks on computer systems. CHIP Unit attorneys are also actively involved in regional training of other prosecutors and federal agents on conducting high-tech investigations, and they work closely with victims of IP theft and cybercrime on prevention efforts.

The combined prosecution efforts of the CHIP network, CHIP Units, and CCIPS create a formidable enforcement network to combat IP crime. These enforcement efforts will be even more critical in the future, as advances in

technology, and the increasingly important role IP plays in the U.S. and global economy, continue to present new challenges.

B. What Is Intellectual Property?

Similar to the way the law recognizes ownership rights in material possessions such as cars and homes, it also grants rights in intangible property, such as the expression of an idea or an invention. Federal law protects IP in four distinct areas: copyright, trademark, patent, and trade secrets.

1. Copyright

Copyright law is designed to foster the production of creative works and the free flow of ideas by providing legal protection for creative expression. Copyright protects the copyright holder against the infringement of any of six exclusive rights in "original works of authorship fixed in any tangible medium of expression," including: computer software; literary, musical, and dramatic works; motion pictures and sound recordings; and pictorial, sculptural, and architectural works. *See* 17 U.S.C. § 102(a). The six exclusive rights are the rights of reproduction, public distribution, public performance, public display, preparation of derivative works, and public performance by digital audio transmission. 17 U.S.C. § 106. Copyright law protects the physical expression of an idea, but not the idea itself. Therefore, legal protection exists as soon as the work is expressed in tangible form, but not before.

Although civil and criminal law contain protections for all the copyright owner's exclusive rights, criminal enforcement focuses primarily on the distribution and reproduction rights, the only two rights for which the violation can be a felony offense subject to higher criminal penalties. *See* 17 U.S.C. § 506(a) and 18 U.S.C. § 2319. Those convicted of criminal felony copyright infringement face up to five years' imprisonment and a $250,000 fine. *Id.*

2. Trademarks and Service Marks

The federal law of trademarks and service marks protects a commercial identity or brand used to identify a product or service to consumers. The Lanham Act, 15 U.S.C. §§ 1051-1127, prohibits the unauthorized use of a trademark, which is defined as "any word, name, symbol, or device" used by a person "to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods." 15 U.S.C. § 1127. By registering trademarks and service marks

with the U.S. Patent and Trademark Office, the owner is granted the exclusive right to use the marks in commerce in the United States, and can exclude others from using the mark, or a comparable mark, in a way likely to cause confusion in the marketplace. A protected mark might be the name of the product itself, such as "Pfizer" or "L.L.Bean", a distinguishing symbol, such as the Nike "Swoosh" or the MGM lion, or a distinctive shape and color, such as the blue diamond shape of a Viagra tablet. Certain symbols like the Olympic rings also receive protection.

Legal protections for trademarks and service marks not only help protect the goodwill and reputation of trademark owners, but also promote fair competition and the integrity of the marketplace. Additionally, they protect consumers by helping to ensure they receive accurate information about the origins of products and services.

Federal criminal law has long prohibited trafficking in goods or services that bear a counterfeit mark. 18 U.S.C. § 2320. As discussed more fully in subsequent chapters, in 2012, the criminal trademark statute was amended to create new offenses and higher penalties for trafficking in counterfeit drugs and certain counterfeit military goods or services. Individuals convicted of § 2320 offenses generally face up to 10 years' imprisonment and a $2 million fine. If the offense involved serious bodily injury, counterfeit drugs, or counterfeit military goods or services, individuals face up to 20 years in prison and a $5 million fine.

3. Patents

Patents protect the world of inventions. In its simplest form, a patent is a property right for an invention granted by the government to the inventor. A patent gives the owner the right to exclude others from making, using, and selling devices that embody the claimed invention. *See* 35 U.S.C. § 271(a). Patents generally protect products and processes, not pure ideas. Thus, Albert Einstein could not have received a patent for his theory of relativity, but methods for using this theory in a nuclear power plant are patentable. Inventors must file for patent protection with the U.S. Patent and Trademark Office.

There are three types of patents: utility, design, and plant. Utility patents are the most common form and are available for inventions that are novel, non-obvious, and useful; that is, "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." 35 U.S.C. § 101. Examples of utility patents include the ingredients

of Silly Putty (1949) and the diagnostic x-ray system known as the CAT-Scan (1975).

Unlike copyright and trademark infringement, there are no criminal—only civil—penalties for committing patent infringement. However, there are some criminal and quasi-criminal penalties for certain conduct related to patents.

4. Trade Secrets

A trade secret can be any form or type of commercially-valuable information that the owner has taken reasonable measures to keep secret and that has an independent economic value from the fact that it is secret and cannot be readily ascertained by the public. Trade secrets can include, for example, technical, scientific, and engineering data, business records, or economic and financial information. *See* 18 U.S.C. § 1839(3). One of the most famous trade secrets is the formula for manufacturing Coca-Cola. The Coca-Cola formula was recognized as a trade secret in 1920, at which time a court noted that the formula had been continuously maintained as a trade secret since the company's founding in 1892. *See Coca-Cola Bottling Co. v. Coca-Cola Co.*, 269 F. 796 (D. Del. 1920) (holding that Coca-Cola retained legal title to its formula upon entering a bottling contract because it kept the formula secret). And, it remains Coca-Cola's most closely guarded trade secret to this day. *See* http://www.worldofcoca-cola.com/secret-vault.htm.

Trade secrets are broader in scope than patents, and include scientific and business information (e.g., market strategies). However, the information can be freely used if it is obtained or learned through legitimate means, such as reverse engineering. Moreover, if the trade secret is publicly disclosed, it generally loses its legal protection.

The theft of trade secrets is punishable by up to 15 years' imprisonment and a $5 million fine if committed to benefit a foreign government or agent, *see* 18 U.S.C. § 1831, and up to ten years' imprisonment and a $250,000 fine in other cases, *see* 18 U.S.C. § 1832.

II. Criminal Copyright Infringement— 17 U.S.C. § 506 and 18 U.S.C. § 2319

Willful copyright infringement is criminalized by 17 U.S.C. § 506(a), which defines what conduct is prohibited, and 18 U.S.C. § 2319, which sets the penalties for such conduct. Felony penalties can attach either when the violation consists of the reproduction or distribution of at least ten copies having a total retail value of at least $2,500 or, under amendments enacted in 2005, when the violation involves online distribution of a "pre-release" work not yet available on the legitimate market over a publicly-accessible computer network.

This Chapter provides an overview of copyright law, an analysis of the elements of copyright infringement, a review of the defenses to the crime, and a summary of the statutory penalties arising from convictions. This chapter also explores some of the novel copyright infringement issues presented by new technologies. Forms providing sample indictments and jury instructions for criminal copyright infringement are provided in Appendix B.

Prosecutors may also wish to consult *Nimmer on Copyright*, a leading treatise on copyright law, with many of its sections being cited by courts as if they were black-letter law, including a chapter on criminal offenses. *See* Melville B. Nimmer & David Nimmer, *Nimmer on Copyright* (2011). Other major treatises and articles that may be instructive include William F. Patry, *Patry on Copyright* (2012); *Copyright Law and Practice* (1994 & Supps. 1995-2000); Ronald D. Coenen Jr. *et al.*, *Intellectual Property Crimes*, 48 Am. Crim. L. Rev. 849 (2011); Michael Coblenz, *Intellectual Property Crimes*, 9 Alb. L.J. Sci. & Tech. 235 (1999).

A. Overview

1. What Copyright Law Protects

In the United States, copyright law has a two-part goal: to protect the rights of authors, and thereby, to foster development of more creative works to benefit the public. The Constitution, in granting Congress the power to enact intellectual property laws, describes this goal and the means to achieve it: "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." U.S. Const., art. I, § 8, cl. 8. Maintaining an appropriate balance between the rights and incentives for authors, and encouraging dissemination of knowledge and information by and to the public, is a constant theme throughout the history of copyright law. *See Twentieth Century Music Corp. v. Aiken*, 422 U.S. 151, 156 (1975).

Copyright law grants the creator of an original work of expression, fixed in a tangible medium, a "copyright," which is the exclusive right, protected for a limited period of time, to copy, distribute, and make certain other uses of the work. *See* 17 U.S.C. § 102(a) (Copyright law protects "*original* works of authorship *fixed in any tangible medium of expression*, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.") (emphasis added). "Originality" in copyright law is a low threshold: the work need only have been independently created by the author, as opposed to copied from another, previous work, and it must possess only a minimal degree of creativity. See Section B.1.a. of this Chapter.

An important limitation of copyright is that it protects *only* the creative expression of an idea, but not the idea itself. See Section B.1.a. of this Chapter. Novel ideas, methods, and processes may enjoy protection under patent law (or other areas of law, such as trade secret protection), but are not copyrightable. For example, consider a microbiologist who invents a new technique for modifying particular genes in a cell, then writes an article for a magazine that describes the technique. The article may be protected by copyright as the author's original expression of his or her ideas regarding this new technique. The technique itself, however, would not be copyrightable, although it may be patentable.

Copyrights are also distinct from trademarks, which protect the exclusive use of certain names, pictures, and slogans used in connection with goods or services. Trademarks need not be original or creative and may consist of short

single words or phrases that are ineligible for copyright protection. Trademarks are discussed in Chapter III of this Manual. Despite the differences between copyrights and trademarks, there are instances in which a single items may be both copyrighted and trademarked; an iconic example of such an item would be the image of Disney's Mickey Mouse.

2. Legal Basis for Copyright and Related Laws

The Constitution grants Congress the power to regulate copyright: "[t]o Promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries," U.S. Const., art. I, § 8, cl. 8. Congress also derives authority to regulate some copyright-related issues from the Commerce Clause, U.S. Const. art. I, § 8, cl. 3.

Copyright protection is principally statutory. *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 429-31 (1984). Federal copyright statutes are found primarily in Title 17 of the U.S. Code, of which sections 101 through 1101 are known as the "Copyright Act," a reference to the last major overhaul of copyright statutes in the 1976 Copyright Act. The offenses for criminal copyright infringement are set forth in 17 U.S.C. § 506 and the related penalties are set forth in 18 U.S.C. § 2319.

The first sale and fair use defenses to copyright infringement, originally common law doctrines, have been codified in the Copyright Act at 17 U.S.C. §§ 107, 109, respectively. Additionally, because courts often interpret copyright law in light of new events and technological developments, there exists significant judge-made law that might not otherwise be obvious from the statutes. *E.g.*, *Metro Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U. S. 913 (2005); *Sony*, 464 U.S. 417.

3. Relevance of Civil Cases to Criminal Prosecutions

The vast majority of copyright case law is civil, rather than criminal, and often civil cases provide the only judicial authority available in criminal prosecutions. In this regard, civil precedent is often instructive to criminal copyright statutes. *See United States v. Wise*, 550 F.2d 1180, 1188 n.14 (9th Cir. 1977) (noting "general principle in copyright law of looking to civil authority for guidance in criminal cases"); *see also United States v. Manzer*, 69 F.3d 222, 227 (8th Cir. 1995) (same); *United States v. Cross*, 816 F.2d 297, 303 (7th Cir. 1987) (same, with respect to jury instructions); *Kelly v. L.L. Cool J.*, 145 F.R.D.

32, 39 (S.D.N.Y. 1992) (noting that conduct that does not support a civil action for infringement cannot constitute criminal infringement); 4 *Nimmer on Copyright* § 15.01.

Criminal penalties, however, apply to only a subset of conduct constituting copyright infringement, and what makes a good civil case does not necessarily make a good criminal case. For example, a defendant can be civilly liable for copyright infringement as a matter of strict liability, with no intent to infringe. *See Bright Tunes Music Corp. v. Harrisongs Music, Ltd.*, 420 F. Supp. 177 (S.D.N.Y. 1976) (finding infringement where composer "subconsciously" copied earlier song). By contrast, a criminal copyright defendant can be convicted only if he infringed willfully. See Section B.2. of this Chapter.

4. Federal Preemption

Copyright law is primarily a matter of federal law. For most of the history of the United States, state- and common-law copyright protections coexisted with federal copyright laws. *See*, *e.g.*, *Wheaton v. Peters*, 33 U.S. 591, 597-98 (1834). But the Copyright Act of 1976 amended Title 17 to preempt state laws that provide rights "equivalent to" rights granted under federal copyright law. 17 U.S.C. § 301(a).

Despite this preemption, copyright law continues to be intertwined with state law in certain cases, such as those involving license agreements and other contracts governing ownership and use of copyrighted works. *E.g., Storage Technology Corp. v. Custom Hardware Eng'g & Consulting, Inc.*, 421 F.3d 1307 (Fed. Cir. 2005). State copyright law also continues to apply to sound recordings recorded before 1972 because sound recordings were not protected by federal copyright law until that year. Consequently, pre-1972 sound recordings may still be protected by state copyrights for several more decades. *See La Cienega Music Co. v. ZZ Top*, 53 F.3d 950 (9th Cir. 1995); 17 U.S.C. § 301(c).

Although § 301 preempts state laws that provide protection equivalent to federal copyright law, a number of states have adopted criminal laws against unauthorized copying or distribution of copies that are directed toward the same types of piracy and counterfeiting targeted by federal criminal copyright laws. For example, most states have adopted statutes (often known as "true names" or "true name and address" laws) that require distributors of copies of certain classes of works (generally recorded music or films) to identify on the copies themselves the name and address of the manufacturer or distributor of those copies. *See*, *e.g.*, Cal. Penal Code § 653w(a)(1) (unlawful to sell recordings

that do not "clearly and conspicuously disclose the actual true name and address of the manufacturer"); Ga. Code § 16-8-60(b) (unlawful to distribute recorded music or film unless copies bear true name and address of producer); Mich. Comp. Laws Ann. § 752.1053 (criminal offense to distribute recordings knowing they do not bear the true name and address of manufacturer); N.Y. Penal Law §§ 275.35, 275.40 (unlawful to commercially distribute recordings that do not bear true name and address of manufacturer or performer); Virginia Code § 59.1-41.4 ("Recorded devices" must show true name of manufacturer).

These types of state law have been upheld against preemption challenges. *See, e.g.*, *Anderson v. Nidorf*, 26 F.3d 100, 102 (9th Cir. 1994) (California "true names" statute not preempted by § 301 in sound recording case); *Briggs v. State*, 638 S.E.2d 292 (Ga. 2006) (Georgia "true names" statute not preempted because lack of identifying label was "extra element" not present in federal copyright law).

5. When Copyright Protection Begins and Ends

A work is protected by copyright law from the moment it is created. *See* 17 U.S.C. §§ 101-102(a), 408(a). Neither publication of the work nor registration of the work with the Register of Copyrights is a prerequisite to copyright *protection*; however, these acts may affect the remedies available for infringement. For example, registration is a prerequisite to a copyright holder's civil suit for infringement, at least in the case of U.S. works. *See* 17 U.S.C. § 411. If a work is registered only after infringement has occurred, a copyright owner may still collect actual damages for infringement committed prior to registration, but cannot collect statutory damages or attorneys' fees. *See* 17 U.S.C. § 412. As clarified in the Prioritizing Resources and Organizations for Intellectual Property (PRO-IP) Act of 2008, Pub. L. No. 110-403, § 101, 122 Stat. 4256, 4257-58 (2008), registration of a copyright is not a prerequisite to criminal prosecution for infringement of that work, although copyright registration is helpful in proving the elements of a criminal case, as discussed in Section B.1. of this Chapter.

Works created in 1978 or later are protected by copyright for the life of the author plus 70 years. *See* 17 U.S.C. § 302(a). For a work with one or more joint authors, the life of the surviving author is used. 17 U.S.C. § 302(b). Works made for hire (i.e., works made by or at the behest of a corporation) and anonymous works are protected for 95 years from the date of first publication, or 120 years from creation (whichever comes first). 17 U.S.C. § 302(c). Most

works created prior to 1978 are protected for 95 years from the date the copyright in the work was first secured (generally the date of publication). 17 U.S.C. § 304.

6. The Rights Protected by Copyright

Copyrighted law grants copyright holders the following six exclusive rights to their works: (1) reproduction, (2) preparation of derivative works based upon the original copyrighted work, (3) public distribution, (4) public performance of certain types of works, (5) public display of certain types of works, and (6) performance of sound recordings by means of digital audio transmission. *See* 17 U.S.C. § 106(1)-(6); 17 U.S.C. § 101 (defining "sound recording" to exclude audiovisual works); 17 U.S.C. § 114(j)(5) (excluding transmission of audiovisual works from the definition of "digital audio transmission"); 17 U.S.C. § 114(d) (limitations including exemptions for certain broadcast transmissions, subscription transmissions, and licensed transmissions). In March 2011, the Office of the Intellectual Property Enforcement Coordinator recommended expanding the performance right in sound recordings to include other, non-digital audio transmissions (such as traditional broadcast radio), and bills have been introduced in Congress to effect similar changes. *See* Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations at 10 (March 2011), *available at* http://www.whitehouse.gov/sites/default/files/ip_white_paper.pdf; Performance Rights Act, H.R. Rep. No. 111-680 (2010) (H.R. 848; S. 379). As of this writing, however, U.S. copyright law grants an exclusive performance right in sound recordings only as to digital audio transmissions.

The exclusive rights set forth in 17 U.S.C. § 106 are subject to a number of exceptions and limitations described in §§ 107-122, such as the right to make limited or "fair use" of a work without permission, to resell or transfer one's own lawful copy of a work, and to reproduce a lawful copy of computer software either as an essential step in using it or to make an archival copy. Those exceptions are addressed throughout this Chapter.

Exercising one of the exclusive rights under § 106 without the copyright holder's authorization, or other legal authority, constitutes copyright infringement. 17 U.S.C. § 501. The exclusive rights granted in § 106 are broad, and include a variety of commercial and noncommercial activities. However, not every unlicensed or unauthorized use of a copyrighted work constitutes an infringement, as many uses will either fall outside the scope of § 106, or be

specifically exempted by §§ 107-122. "An unlicensed use of the copyright is not an infringement unless it conflicts with one of the specific exclusive rights conferred by the copyright statute." *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 447 (1984) (citation omitted); *see also* Benjamin Kaplan, *An Unhurried View of Copyright* 57 (1967) ("The fundamental [is] that 'use' is not the same thing as 'infringement,' that use short of infringement is to be encouraged ....").

7. When Infringement Is Criminal

Any instance of infringement will generally entitle a copyright owner to a civil remedy, such as damages or injunctive relief. But not every infringement is a criminal offense. Throughout the history of copyright in the United States, criminal copyright penalties have been the exception rather than the rule. Although criminal copyright law has greatly expanded the scope of the conduct it penalizes over the past century, criminal sanctions continue to apply only to certain types of infringement—generally when the infringer knows the infringement is wrong, and when the infringement is particularly serious or the type of case renders civil enforcement by individual copyright owners especially difficult. As described in more detail below, a willful violation of any exclusive right for commercial advantage or private financial gain is a misdemeanor, whereas only a violation of the rights to reproduction and distribution under certain circumstances constitutes felony infringement.

Copyright infringement is a crime if the defendant infringed *willfully* and did so either (1) for commercial advantage or private financial gain, (2) by reproducing or distributing one or more infringing copies of works with a total retail value of over $1,000 over a 180-day period, or (3) by distributing a "work being prepared for commercial distribution" by making it available on a publicly-accessible computer network. 17 U.S.C. § 506(a)(1). Criminal copyright infringement is punishable as a felony if the criminal conduct described above involved reproduction or distribution of at least ten copies of copyrighted works worth more than $2,500 in a 180-day period, or involved distribution of a "work being prepared for commercial distribution" over a publicly-accessible computer network. *See id.*; 18 U.S.C. § 2319.

B. Elements

There are three essential copyright crimes:

1. Willful infringement "for purposes of commercial advantage or private financial gain," 17 U.S.C. § 506(a)(1)(A).
2. Willful infringement by "the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000," 17 U.S.C. § 506(a)(1)(B). Note that this type of infringement does not have a financial component.
3. Willful infringement "by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution," 17 U.S.C. § 506(a)(1)(C) (enacted in 2005). This violation, enacted in 2005, is commonly referred to as "pre-release" piracy and also does not have a financial component.

The common factors for all criminal copyright offenses are that (1) there must be a valid copyright, (2) there must be an infringement, and (3) the infringement must be willful. Some courts also require that the government prove an extra element: that the infringing items at issue were not permissible "first sales," although most courts hold the issue of "first sale" to be an affirmative defense. See Section C.4. of this Chapter.

Felony copyright infringement only occurs when the defendant willfully infringed a copyright by reproduction and distribution and only in the following ways:

1. by (a) reproducing or distributing, "including by electronic means;" (b) "during any 180-day period;" (c) "at least 10 copies or phonorecords, of 1 or more copyrighted works;" (d) that have a "total retail value of more than $2,500." 18 U.S.C. § 2319(b)(1); OR
2. by (a) distributing a work; (b) that is "being prepared for commercial distribution;" (c) by "making it available on a computer network;" (d) "[knowing it] was intended for commercial distribution." 17 U.S.C. § 506(a)(1)(C); 18 U.S.C. § 2319(d).

Although felony copyright infringement does not require a profit motive, the maximum penalties will increase from three years to five if the offense is committed for commercial advantage or private financial gain. 18 U.S.C. §§ 2319(b)(1), (d)(2).

In other words, there are four essential elements to a charge of *felony* copyright infringement:

1. A valid copyright exists (see Section B.1. of this Chapter);
2. The defendant acted willfully (Section B.2. of this Chapter);
3. The defendant infringed the copyright by reproduction or distribution of the copyrighted work, or for violations of 17 U.S.C. § 506(a)(1)(C), by distribution (Section B.3.a. of this Chapter);
4. The infringement consisted of either of the following:
   (a) reproduction or distribution of at least 10 copies of one or more copyrighted works with a total retail value of more than $2,500 within a 180-day period (Section B.3.b. of this Chapter); OR
   (b) distribution
      (i) of copies of a "work being prepared for commercial distribution"
      (ii) by making such copies available on a publicly-accessible computer network
      (iii) when the defendant knew or should have known the work was being prepared for commercial distribution (Section B.3.c. of this Chapter).

Repeat felonies are subject to increased maximum penalties. *See* 18 U.S.C. § 2319(b)(2), (c)(2), (d)(3)-(4).

Amendments to the criminal copyright statutes in 1997 and 2005 significantly changed the elements of felony copyright infringement. *See* No Electronic Theft Act (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997) (removing the financial requirement for felony infringement); Family Entertainment and Copyright Act of 2005, Pub. L. No. 109-9 § 103, 119 Stat. 218, 220-21 (2005) (creating a felony for pre-release piracy and camcording in a movie theater, among other things); *see also* Prioritizing Resources and Organizations for Intellectual Property (PRO-IP) Act of 2008, Pub. L. No. 110-403, 122 Stat. 4256 (2008) (clarifying forfeiture authority for property

used to facilitate criminal copyright and other intellectual property offenses). Cases predating these statutes should not necessarily be relied upon for delineating the elements of current copyright offenses, but they remain useful in interpreting the current law's elements.

1. Existence of a Copyright

Under 17 U.S.C. § 506(a), the initial element of criminal copyright infringement is that a valid copyright exists in the work or works in question. While on its face this element may appear the simplest to prove, a number of issues can add considerable complexity.

a. Copyrightability

Copyright law protects all "*original* works of authorship *fixed in any tangible medium of expression* ...." 17 U.S.C. § 102(a) (emphasis added).

i. Original Work Fixed in a Tangible Medium

The subject matter of copyright is defined by two requirements: originality and fixation. A work must be an original, creative expression of an idea or concept, and it must be recorded in tangible form. Thus, copyright law protects a novel or poem written on paper or typed in a computer, a song recorded in a studio or written on sheet music, a sculpture modeled in clay or bronze, or a computer program on a computer's hard disk.

For copyright purposes, "original" has two requirements. First, the work must have been independently created by the author, as opposed to copied from another previous work. A work can be original even if it closely resembles another work, "so long as the similarity is fortuitous, not the result of copying." *Feist Publ'ns, Inc. v. Rural Telephone Co.*, 499 U.S. 340, 345-46 (1991) (citing *Sheldon v. Metro-Goldwyn Pictures Corp.*, 81 F.2d 49, 54 (2d Cir. 1936) (noting that identical poems created by different poets ignorant of one another would both be original and copyrightable)). In practice, the odds against an artist or author or musician creating a new work identical to an existing one, without knowing of the earlier work, are remote, and in cases involving suspiciously-similar works, where the later artist had access or opportunity to learn of the earlier work, courts have found the subsequent work infringing. *See*, *e.g.*, *Bright Tunes v. Harrisongs Music*, 420 F. Supp. 177 (S.D.N.Y. 1976). Second, the work must also possess "at least some minimal degree of creativity." *Feist*, 499 U.S. at 345. The amount of creativity required for originality is extremely low;

"a slight amount" of "creative spark" is all that is necessary, "no matter how crude, humble or obvious." *Id.* (citing 1 *Nimmer on Copyright* §§ 2.01[A], [B] (1990)). What qualifies as "original" for copyright purposes may not be considered "original" by, for example, those assessing the item's artistic, literary, or academic merit. Nor should "originality" be confused with "novelty," which is the touchstone of patent law, not copyright. See Chapter VII of this Manual.

To be copyrightable, a work must also be "fixed," meaning the work is recorded in some tangible medium by the author. For example, a song that is composed onto sheet music or recorded to tape is fixed and thus copyrightable, but a live performance of a song that is not recorded by the performer (or someone authorized by the performer) would not be fixed, and thus the performance itself would not be copyrightable, although the performance might still enjoy protection under other laws. See the discussion of 18 U.S.C. § 2319A in Section F. of this Chapter.

ii. Short Phrases Are Not Copyrightable

Short single words, short phrases, and familiar symbols and designs generally cannot be copyrighted. 37 C.F.R. § 202.1(a) (2004). They may, however, be trademarked and thus protected under 18 U.S.C. § 2320; see Chapter III of this Manual.

iii. Expression of an Idea vs. Idea Itself

An important limitation of copyright is that it protects *only* the creative expression of an idea—but not the idea itself. 17 U.S.C. § 102(b) ("In no case does copyright protection ... extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery ...."); *see also Feist*, 499 U.S. at 344-45; *Mannion v. Coors Brewing Co.,* 377 F. Supp. 2d 444 (2005); *Whelan Assoc. v. Jaslow Dental Lab.*, 797 F.2d 1222 (3d Cir. 1986). Novel ideas, methods, and processes may enjoy protection under trade secret or patent law, but are not copyrightable. See Chapters IV and VII of this Manual. For example, consider a new technique for modifying genes in a cell that is described in a magazine article. Although the *article* might be copyrightable—as an original expression of the author's ideas about this new technique—the *technique* itself would not. The technique might, however, be patentable.

b. Copyrights vs. Registrations vs. Certificates

The notion of having a valid copyright is easily confused with the issue of whether the work is *registered* with the Copyright Office, or with possession of a valid copyright *certificate* issued by the Copyright Office. Throughout much of U.S. history, copyright protection was predicated on certain formal requirements, such as the need to register published works with the Copyright Office, deposit copies with the Library of Congress, and mark copies of the work with a copyright notice. However, major revisions to copyright law in the 1970s and 1980s eased these requirements, and now protect a copyrightable work regardless of whether such formalities have been observed. *See La Resolana Architects, PA v. Clay Realtors Angel Fire*, 416 F.3d 1195, 1198-1205 (10th Cir. 2005), *abrogated on other grounds by Reed Elsevier, Inc. v. Muchnick*, 130 S.Ct. 1237 (2010). For a work created on or after January 1, 1978, copyright subsists from the moment an original work of authorship is created by "fix[ing it] in any tangible medium of expression." 17 U.S.C. § 102(a); *see also id.* § 302(a). That is, a work is copyrighted the moment it is created, regardless of whether it has been registered or bears a copyright notice.

A "copyright" is the author's legal entitlement to the exclusive rights granted under 17 U.S.C. § 106. Neither a copyright registration nor a registration certificate is equivalent to a copyright. A registration certificate signifies the Copyright Office's decision to register the work, which is a limited administrative decision that the work is copyrightable subject matter and that the application is proper. *See* 17 U.S.C. § 408(a). Although not dispositive of whether a valid copyright exists, the Copyright Office's decision to issue a registration and the certificate of registration can, however, have legal significance at trial. See Sections B.1.d.-e. of this Chapter.

c. "Preregistration" of Certain Types of Works

The Family Entertainment and Copyright Act of 2005 created a new procedure, known as "preregistration," intended to address some problems with works that are pirated before their lawful publication or official release by the copyright owner. *See* Pub. L. No. 109-9 § 104, 119 Stat. 218, 221-22 (Apr. 27, 2005); 17 U.S.C. §§ 408(f) (setting forth basic rules for preregistration), 411(a) (preregistration or registration necessary to institute infringement action in most cases); 37 C.F.R. § 202.16 (Copyright Office rules for preregistration). Preregistration is available for certain types of work judged by the Copyright Office to be especially vulnerable to piracy before their lawful release or

publication, including movies, musical compositions and sound recordings, computer software and video games, literary works, and "advertising and marketing photographs." *See id*. A copyright owner can preregister these types of works if they are unpublished, but "being prepared for commercial distribution," meaning that the copyright owner has a reasonable expectation that the work will be commercially distributed to the public, and the work, if not yet finished, has at least been commenced. *Id.* § 202.16(b)(2). Upon submission of an application and fee, the Copyright Office will undertake a limited review of the work, and if approved, it will preregister the work and issue a certificate, much as in the case of copyright registration. *Id.* § 202.16(c).

But preregistration is not a complete substitute for registration. Although preregistration offers some benefits to copyright owners, preregistration involves only a cursory review by the Copyright Office and consequently preregistration, unlike registration, will *not* serve as *prima facie* evidence of the validity or ownership of a copyright. 37 C.F.R. § 202.16(c)(6), (7), (13). See Sections B.1.d.-e. of this Chapter.

d. Significance of Registration

As noted above, a creative work can be *protected* by copyright even before, or absent, registration of the work with the Copyright Office. Many foreign works of authorship are never registered with the United States Copyright Office, nor are most unpublished works by domestic authors ever registered, and yet such works may still enjoy copyright protection under U.S. law. However, registration of a copyright may be necessary for a copyright owner to *enforce* such protections civilly. Specifically, U.S. law requires copyright owners to register their works with the Copyright Office as a prerequisite to filing a lawsuit for infringement. Section 411 of Title 17 provides that "no *civil* action for infringement of the copyright in any United States work shall be instituted until preregistration or registration of the copyright claim has been made in accordance with this title." § 411(a) (emphasis added). Note that § 411 applies only to "United States work[s]," meaning works first published domestically, or works created by U.S. nationals or "habitual residents." *See* 17 U.S.C. §§ 101, 411(a). Thus, before a civil lawsuit for infringement of a United States work can be initiated, the work must be registered, although registration is not a prerequisite to filing a law suit for infringement of a *foreign* work (nor is registration a prerequisite for criminal enforcement, as discussed below).

Some aspects of the § 411 registration requirement are the subject of disagreements among the federal courts. For example, courts continue to disagree over which specific steps § 411 requires to be satisfied prior to the filing of a lawsuit. Although some courts require only that a copyright owner submit a facially valid application and required fee to the Copyright Office before filing suit, most conclude that § 411's language (that a registration must be "made" prior to suit) means the Copyright Office must have either accepted and approved the registration, or formally rejected it as invalid, prior to the filing of a lawsuit. *Compare Lakedreams v. Taylor*, 932 F.2d 1103, 1108 (5th Cir. 1991) (Section 411 requires only the filing of an application before suit may be filed); *Apple Barrel Prods., Inc. v. Beard*, 730 F.2d 384, 386-87 (5th Cir. 1984) (same); *Prunte v. Universal Music Group*, 484 F. Supp. 2d 32 (D.D.C. 2007) (same) *with La Resolana Architects, PA v. Clay Realtors Angel Fire*, 416 F.3d 1195 (10th Cir. 2005) (Section 411 requires Copyright Office to issue or reject registration prior to filing of lawsuit), *abrogated on other grounds by Reed Elsevier, Inc. v. Muchnick*, 130 S.Ct. 1237 (2010); *M.G.B. Homes, Inc. v. Ameron Homes, Inc.*, 903 F.2d 1486, 1488 (11th Cir. 1990); *Mays & Assocs. Inc. v. Euler, Inc.,* 370 F. Supp. 2d 362, 368 (D. Md. 2005) (Section 411 requires registration as opposed to mere application for copyright); *see also Vacheron & Constantin-Le Coultre Watches, Inc. v. Benrus Watch Co.*, 260 F.2d 637, 640-41 (2d Cir. 1958) (filing of suit under pre-1976 law requires that registration process be complete).

The Supreme Court in *Reed Elsevier, Inc. v. Muchnick*, 130 S. Ct. 1237 (2010) resolved another circuit split over the issue of whether registration is, on the one hand, merely a procedural requirement or case-processing rule, or whether, on the other hand, is necessary to confer subject-matter jurisdiction in federal court. Reversing the Second Circuit, the Supreme Court held that although registration is a precondition to filing an action in district court, failure to comply with § 411 does not deprive a federal court of subject matter jurisdiction to hear claims involving unregistered works. The Court, however, declined to address whether registration is a threshold mandatory requirement that district courts may or should enforce by dismissing *sua sponte* cases involving unregistered works.

i. Registration Not a Prerequisite for Criminal Prosecution

Copyright registration is not a prerequisite to a criminal prosecution for copyright infringement. The Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP) Act of 2008, Pub. L. No. 110-403,

122 Stat. 4256 (2008) clarified this point by amending § 411 to add the word "civil." Notwithstanding that copyright registration is not a requirement for initiating a criminal prosecution, copyright registration is nevertheless helpful in proving certain elements of the offense at trial and avoiding a number of practical challenges that may result from a lack of registration. See Section B.2.b. of this Chapter. For example, introducing certificates of registration at trial is often the simplest way to prove a copyright's validity and ownership. Even though registration is not legally required, without it prosecutors will have to prove these elements "from scratch" through testimony and other evidence. See Section B.1.e. of this Chapter. Therefore, to the extent possible, prosecutors should try to ensure that any copyrights on which a prosecution is sought are registered or "preregistered" before the prosecution is commenced. If registration is needed for pending litigation, it can often be expedited for completion within a week. *See* U.S. Copyright Office, Information Circular 10, "Special Handling," *available at* http://www.copyright.gov/circs/circ10.pdf.

Copyright certificates or completed registrations are useful prior to trial, but not as critical. So long as the government can present sufficient evidence of a valid copyright to satisfy a probable cause standard, a lack of a copyright registration or certificate should not be an impediment to obtaining search warrants, grand jury subpoenas, and even indictments.

When registration is lacking (which may merely be an oversight, or could reflect a conscious choice to delay registration until a work is ready for publication) prosecutors should bear in mind the circumstances surrounding the absence of registration, which may militate against the choice to prosecute. For example, a copyright-holder's refusal to register his copyright may indicate—or be interpreted as—his intent to allow others to copy the work. If, on the other hand, registration has been sought from the Copyright Office and refused, the refusal may indicate a weak claim of copyrightability or ownership.

e. Proof of Copyright at Trial

At trial, the government typically proves the existence of a valid copyright by introducing a certificate of registration. The certificate's probative value depends on whether the work was registered earlier or later than five years after the work was published. A certificate of registration "made before or within five years after first publication of the work shall constitute *prima facie evidence* of the validity of the copyright." 17 U.S.C. § 410(c) (emphasis added); *see Gaylord*

v. United States, 595 F.3d 1364, 1376 (Fed. Cir. 2010)*; United States v. Taxe*, 540 F.2d 961, 966 (9th Cir. 1976); *United States v. Moore*, 604 F.2d 1228, 1234 (9th Cir. 1979); *see also* 17 U.S.C. § 101 ("'Publication'" is the distribution of copies or phonorecords of a work to the public by sale or other transfer of ownership, or by rental, lease, or lending. The offering to distribute copies or phonorecords to a group of persons for purposes of further distribution, public performance, or public display, constitutes publication. A public performance or display of a work does not of itself constitute publication.").

Once the certificate of registration is introduced by the government and accepted as authentic by the court, the burden shifts to the defendant to prove that the copyright is not valid or that the registration was obtained fraudulently. *See, e.g.*, *Gaylord*, 595 F.3d at 1376; *Autoskill, Inc. v. Nat'l Educ. Support Sys., Inc.*, 994 F.2d 1476, 1487 (10th Cir. 1993), *overruled on other grounds by TW Telecom Holdings Inc. v. Carolina Internet Ltd.*, 661 F.3d 495 (10th Cir. 2011). Then, the prosecutor may rebut with evidence showing that the certificate is genuine, the registration was properly obtained, or that the copyright is otherwise valid. If the work was registered more than five years after its first publication, the certificate's probative value is left to the court's discretion. *See* 17 U.S.C. § 410(c); *Religious Tech. Ctr. v. Netcom On-Line Comm. Servs., Inc.*, 923 F. Supp. 1231, 1241 (N.D. Cal. 1995); *Pan-American Products & Holdings, LLC v. R.T.G. Furniture Corp.*, 825 F. Supp. 2d 664, 702 (M.D.N.C. 2011); *Koontz v. Jaffarian*, 617 F. Supp. 1108, 1111-12 (E.D. Va. 1985), *aff'd*, 787 F.2d 906 (4th Cir. 1986).

Certificates of registration should be obtained from the victim. The Copyright Office has an online database of certifications and can provide certified copies. *See* http://www.copyright.gov/records/; U.S. Copyright Office, Information Circular No. 6, "Obtaining Access to and Copies of Copyright Office Records and Deposits," *available at* http://www.copyright.gov/circs/circ06.pdf. But copyright owners may be able to respond faster, since they should have retained their registration certificates in the ordinary course of their business.

Although producing a copyright certificate is the preferred method of proving validity and ownership of a valid copyright, it is not the only way to do so. The parties can stipulate to the copyright's validity. *E.g.*, *United States v. Beltran*, 503 F.3d 1, 2 (1st Cir. 2007); *United States v. Sherman*, 576 F.2d 292, 296 (10th Cir. 1978). Courts may also take judicial notice of a work's copyright registration. *Island Software and Computer Service, Inc. v. Microsoft*

Corp., 413 F.3d 257, 261 (2d Cir. 2005); *see also United States v. Hux*, 940 F.2d 314, 318 (8th Cir. 1991) (allowing introduction of copyright certificates the morning of trial, but noting other evidence previously given to defense provided ample basis for plaintiff to establish, and defendant to challenge, existence of copyright), *overruled on other grounds by United States v. Davis*, 978 F.2d 415 (8th Cir. 1992); *La Resolana Architects, PA*, 416 F.3d at 1208; *United States v. Backer*, 134 F.2d 533, 535-36 (2d Cir. 1943) (allowing civil proceeding where Copyright Office had provided plaintiff with certificate due to error; technical irregularities in the registration process should not invalidate an otherwise proper registration). For instance, the government could introduce testimony regarding the copyright owner's creation and fixation of the work, evidence that the work is original, and that it was not a work for hire created for someone else.

In cases where the validity of a copyright is likely to be contested, prosecutors may wish to gather additional evidence of the validity of the copyright, such as the type described above. Even where copyright in a work has been registered within five years of publication thus giving rise to a presumption of validity, some courts have cautioned against placing too much weight on registrations as proof of a valid copyright, due to the cursory nature of the copyright registration process. *See Universal Furniture Int'l, Inc. v. Collezione Europa USA, Inc.*, 618 F.3d 417, 428 (4th Cir. 2010); *Charles W. Ross Builder, Inc. v. Olsen Fine Home Bldg., LLC*, 827 F. Supp. 2d 607, 616 (E.D. Va. 2011); *Pan-American Products*, 825 F. Supp. 2d at 702.

f. Copyright Notice

Particularly in cases involving older works, prosecutors should confirm that copyright in a work has not lapsed. Copyright protection expires at the end of the statutory term, which will vary depending on the date of creation, publication, or the author's death. However, for works first published prior to March 1, 1989, copyright may also have lapsed if the work lacked a valid copyright notice upon its first publication. For works published on or after March 1, 1989, their publication without a copyright notice is of no moment. *See* Berne Convention Implementation Act of 1988 ("BCIA"), Pub. L. No. 100-568, 102 Stat. 2853 (enacted October 31, 1988). For works published before March 1, 1989, however, initial publication without a copyright notice would have extinguished their copyright and consigned them to the public domain. *See* 17 U.S.C. §§ 10, 19 *et seq*. (1909 Act); 17 U.S.C. § 405(a)(2) (1976 Act); *see also* 2 *Nimmer on Copyright* §§ 7.02[C][1]-[3], at 7-16 to 7-17.

Generally speaking, the form of copyright notice generally contains the symbol ©, the word "copyright," and the name of the copyright owner (e.g., Copyright © 2011 by Jane Doe).

As noted in the following Section, the presence of a copyright notice on an infringed work may be useful in proving a defendant's willfulness.

2. The Defendant Acted "Willfully"

a. Legal Standard

To establish criminal intent, the government must prove that the defendant infringed the copyright *willfully*. *See* 17 U.S.C. § 506(a) ("Any person who *willfully* infringes a copyright shall be punished ....") (emphasis added). "[E]vidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement." 17 U.S.C. § 506(a)(2). This was intended to require proof of more than general intent and to ensure that, for instance, "an educator who in good faith believes that he or she is engaging in a fair use of copyrighted material could not be prosecuted under the bill." 143 Cong. Rec. 26,420-21 (1997).

The Supreme Court has recognized that "willful ... is a word of many meanings, its construction often being influenced by its context." *Spies v. United States*, 317 U.S. 492, 497 (1943). This was reflected in Congressional debate over the NET Act amendments to the Copyright Act. Senator Hatch, the Chairman of the Senate Judiciary Committee, advocated that in copyright crimes "'willful' ought to mean the intent to violate a known legal duty," 143 Cong. Rec. 26,420 (1997), because a lower *mens rea* could cause "the net" of criminal sanctions "[to] be cast too widely." *Id*. Senator Hatch cited several cases in which the Supreme Court had construed "willfulness" in this fashion when the substantive law was complex, such as *Cheek v. United States*, 498 U.S. 192 (1991), in which the Court held that the general principle that "ignorance of the law or a mistake of law is no defense to criminal prosecution," must yield given the complexity of federal criminal tax statutes. In other words, the defendant's good-faith misunderstanding of the legal duties imposed on him by the tax laws would negate a finding of willfulness. *Id.* at 199. This reasoning has been applied in other contexts as well. *E.g.*, *Ratzlaf v. United States*, 510 U.S. 135 (1994) (failure to report cash transactions in excess of $10,000).

In debate on the corresponding House bill, two of the bill's sponsors, Representatives Goodlatte and Coble, made comments suggesting that

the "willfulness" may be met with something less than direct proof that the defendant was actually aware he was violating the law:

> It should be emphasized that proof of the defendant's state of mind is not required. The Government should not be required to prove that the defendant was familiar with the criminal copyright statute or violated it intentionally. Particularly in cases of clear infringement, the willfulness standard should be satisfied if there is adequate proof that the defendant acted with reckless disregard of the rights of the copyright holder. In such circumstances, a proclaimed ignorance of the law should not allow the infringer to escape conviction. Willfulness is often established by circumstantial evidence, and may be inferred from the facts and circumstances of each case.

143 Cong. Rec. 24,325 (1997) (statement of Rep. Coble); *see also id.* at 24,326 (statement of Rep. Goodlatte, repeating passage above verbatim, with the addition of the word "also" after "be" in the first sentence). Although the first sentence of the passage quoted above might suggest Representatives Coble and Goodlatte viewed the criminal copyright offense as a strict liability crime, the context of their statements suggests that both Congressmen meant, not that the criminal copyright offense required *no* proof of a defendant's intent or state of mind, but rather that the "willfulness" standard did not require *direct* evidence of *mens rea*, and that a "willful" state of mind could be proven circumstantially (or, in their view, through affirmative proof of reckless disregard for the rights of copyright holders).

Although the statements of individual members reflect somewhat differing conceptions of the "willfulness" standard, both houses of Congress indicated their intent not to affect the existing "willfulness" standard applicable to copyright crime, other than to clarify that evidence of reproduction or distribution, by itself, was insufficient to prove willfulness. *See* 17 U.S.C. § 506(a)(2); Statement of Rep. Coble, 143 Cong. Rec. 24,325 (1997) ("Evidence of reproductions or distributions, including those made electronically on behalf of third parties, would not, by itself, be sufficient to establish willfulness under the NET Act."). Otherwise, Congress left the term's definition to the courts. *See* 143 Cong. Rec. 26,422 (remarks of Sen. Leahy) ("This clarification does not change the current interpretation of the word 'willful' as developed by case law and as applied by the Department of Justice, nor does it change the definition of 'willful' as it is used elsewhere in the Copyright Act."); H.R. Rep.

No. 102-997, at 4-5 (1992), *reprinted in* 1992 U.S.C.C.A.N. 3569, 3572-73 (discussion of Copyright Felony Act, Pub. L. No. 102-561, 106 Stat. 4233 (1992)).

Most courts that have interpreted "willfulness" in criminal copyright cases have adopted the more stringent standard articulated by Senator Hatch: the intentional violation of a known legal duty. *See United States v. Moran*, 757 F. Supp. 1046, 1049 (D. Neb. 1991) (holding that willful infringement means a "'voluntary, intentional violation of a known legal duty'") (quoting *Cheek v. United States*, 498 U.S. 192, 200 (1991)); *see also United States v. Sherman*, 576 F.2d 292, 297 (10th Cir. 1978) (upholding jury's verdict because jury "apparently either disbelieved the genuineness of this contract [which defendants claimed had licensed their conduct], or believed that defendants were not innocent of knowledge that the tapes provided were copies from the original artists' records", and noting that "willfulness" required proof of specific intent, but without clarifying whether that required proof that the defendants knew their conduct was unlawful, or merely knowledge that they were selling copies); *cf. United States v. Heilman*, 614 F.2d 1133, 1138 (7th Cir. 1980) (holding that the government had proved willfulness because the defendant "chose to persist in conduct which he knew had 'a high likelihood of being held by a court of competent jurisdiction to be a violation of a criminal statute'") (quoting trial court); *United States v. Cross*, 816 F.2d 297, 300-01 (7th Cir. 1987) (approving without comment a jury instruction that an act is willful when it is committed "voluntarily, with knowledge that it was prohibited by law, and with the purpose of violating the law, and not by mistake, accident or in good faith," and affirming conviction because the record amply demonstrated that the defendant "knowingly and voluntarily violated the copyright laws"); *see also* Ronald D. Coenen Jr. et al., Intellectual Property Crimes, 48 Am.Crim. L.Rev. 849, 877-89 (2011).

A minority of courts in criminal copyright cases have suggested that a lower standard of "willfulness" may support a criminal prosecution. *United States v. Backer*, 134 F.2d 533, 535 (2d Cir. 1943) is frequently cited as applying the lower standard, that of merely having the intent to carry out the activities of infringement without knowledge that they constituted infringement. In that case, the defendant had arranged for a manufacturer to duplicate a copyrighted figurine as closely as possible without, in the defendant's words, "copyright trouble." *Id.* at 535. The Second Circuit found the evidence sufficient to support willful infringement, noting there could not "be any fair doubt that

the appellant deliberately had the copies made and deliberately sold them for profit." *Id*. Some commentators have characterized *Backer* as representing a circuit split. *E.g.*, 4 *Nimmer on Copyright* § 15.01[A][2] at 15-6 (opining that "[T]he better view construes the 'willfulness' required for criminal copyright infringement as a 'voluntary, intentional violation of a known legal duty.'"); Julie L. Ross, *A Generation of Racketeers? Eliminating Civil RICO Liability for Copyright Infringement*, 13 Vand. J. Ent. & Tech. L. 55, 85 (2010); Mary Jane Saunders, *Criminal Copyright Infringement and the Copyright Felony Act*, 71 Denv. U. L. Rev. 671, 673 (1994).

It is not clear, however, that *Backer* represents an actual circuit split. The case can also be read as holding the defendant's mention of "copyright trouble" to be sufficient evidence of his knowledge of a legal duty not to infringe. Moreover, more recent civil copyright cases suggest that the Second Circuit interprets willfulness to require either actual knowledge that the infringement violated the law, or perhaps "constructive knowledge" shown by reckless disregard for whether the conduct violated copyright. *See Twin Peaks Prods., Inc. v. Publ'ns Int'l, Ltd.*, 996 F.2d 1366, 1382 (2d Cir. 1993) (holding standard for willfulness to be "whether the defendant had knowledge that its conduct represented infringement or perhaps recklessly disregarded the possibility"); *Fitzgerald Publ'g Co. v. Baylor Publ'g Co.*, 807 F.2d 1110, 1115 (2d Cir. 1986) (same); Lydia Pallas Loren, *Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and The Importance of the Willfulness Requirement*, 77 Wash. U. L.Q. 835, 879 (1999) (arguing that the Second Circuit is actually not in disagreement with other circuits). This approach is consistent with the Seventh Circuit's ruling in *United States v. Heilman*, a criminal copyright case holding that the government proved willfulness because the defendant "chose to persist in conduct which he knew had a high likelihood of being held by a court of competent jurisdiction to be a violation of a criminal statute." 614 F.2d 1133, 1138 (7th Cir. 1980) (citation and internal quotation marks omitted).

The majority rule in criminal copyright cases for a higher standard of willfulness is also generally consistent with civil copyright cases. The issue arises in civil cases when plaintiffs attempt to recover increased statutory damages, which are available only for willful infringement. 17 U.S.C. § 504(c). Whereas criminal willfulness requires a specific intent to violate "a known legal duty," civil cases require a more specific intent to violate copyright laws; that is that willfulness is not just an intent to copy, but rather an intent to infringe. 4

Nimmer on Copyright § 14.04[B][3][a]; *e.g.*, *BC Technical, Inc. v. Ensil Int'l Corp.*, 464 Fed. Appx. 689 (10th Cir. 2012) ("willful" infringement in civil case requires specific intent to violate copyright laws - also noting without analysis that criminal cases require an intent to violate copyright laws, but relying, in part, on criminal cases and authorities referring to "known legal duty"); *Twin Peaks Prods., Inc.*, 996 F.2d at 1382; *Danjaq, L.L.C. v. Sony Corp.*, 263 F.3d 942, 959 (9th Cir. 2001); *RSO Records, Inc. v. Peri*, 596 F. Supp. 849, 859 (S.D.N.Y. 1984) (holding, in civil action, that defendant's earlier guilty plea to two counts of criminal copyright infringement sufficed to show he knew similar conduct was unlawful). Given that willfulness requires an intent to infringe, or at least constructive knowledge of infringement plus a reckless disregard of the victim's rights, a finding of willfulness may be precluded if the defendant acted with a good-faith belief that he was not infringing. See Section B.2.b. of this Chapter.

b. Proof at Trial

"Willfulness is rarely provable by direct evidence, and most often can be proven only by inference from the evidence introduced." *United States v. Sherman,* 576 F.2d at 297. Certain types of evidence in criminal copyright cases have been found particularly relevant to proving the defendant's intent:

- **The defendant's acknowledgment that his or her conduct was improper.** *See United States v. Manzer*, 69 F.3d 222, 227-28 (8th Cir. 1995) (defendant's admission in a published interview that selling or giving away copyrighted computer chips was illegal, and software program and packaging bore copyright notice); *United States v. Drebin*, 557 F.2d 1316, 1324 (9th Cir. 1977) (defendant's warning customers of FBI investigation and recommending that customers "really be careful"); *United States v. Hux*, 940 F.2d 314, 319 (8th Cir. 1991) (defendant's admission to FBI that he knew modifying copyrighted descrambler chips was infringement), *overruled on other grounds by United States v. Davis*, 978 F.2d 415 (8th Cir. 1992); *United States v. Taxe*, 540 F.2d 961, 968-69 (9th Cir. 1976) (defendant's solicitation of attorney to lie about legality of tapes); *United States v. Kim*, 307 Fed. Appx. 324, 326 (11th Cir. 2009) (statements by CEO to buyers from which CEO's willful intent and awareness of unlawfulness "reasonably could be inferred").

- **Actual notice to the defendant that his own conduct was illegal.** *See, e.g., United States v. Cross*, 816 F.2d 297, 300-01 (7th Cir. 1987) (defendant's sale of pirated videotapes after FBI agents told him that selling and renting unauthorized tapes was illegal). Cease and desist letters from rights owners to the defendant can also be useful in establishing willfulness.
- **Notice to the defendant that another person's similar conduct constituted infringement.** *See United States v. Heilman*, 614 F.2d 1133, 1138 (7th Cir. 1980) (defendant's awareness that government was prosecuting individuals engaged in conduct similar to his own and that conduct had been ruled illegal by four federal and three state courts); *United States v. Kim*, 307 Fed. Appx. 324 (11th Cir. 2009) (not error for court to find defendant acted willfully where there was evidence that defendant's cousin, a police officer, had advised his conduct was illegal and defendant had previously been convicted of trademark counterfeiting).
- **The defendant's past manufacture and distribution of infringing items.** *See United States v. Kim*, 307 Fed. Appx. 324 (11th Cir. 2009) (not error for court to find defendant acted willfully where defendant had previously been convicted of trademark counterfeiting, and had been advised by police officer relative that his conduct was illegal); *United States v. Whetzel*, 589 F.2d 707, 712 (D.C. Cir. 1978), *abrogated on other grounds*, *Dowling v. United States*, 473 U.S. 207 (1985).
- **The defendant's admission to copying, in conjunction with other circumstantial evidence indicating defendant knew copies were unauthorized.** *United States v. Dadamuratov*, 340 Fed. Appx. 540 (11th Cir. 2009) (admission of copying, along with circumstantial evidence of infringement and knowledge, sufficient to prove willful infringement).
- **The defendant's statement to Postal Service employee that others were selling illegal DVDs in the area.** *United States v. Draper*, No. 7-05 CR 0004, 2005 WL 2746665, at *2 (W.D. Va. Oct. 24, 2005).
- **The defendant's frivolous or bad-faith claim of compliance with copyright laws, which demonstrates knowledge of copyright laws.** *Cf. United States v. Gardner*, 860 F.2d 1391, 1396 (7th Cir. 1988) (holding that when seller of "black boxes" for receiving unauthorized

cable TV gave buyers a "Notice of Warning" that disclaimed liability for illegal uses, it was "establish[ed] that he was well aware that his actions were unlawful").

- **The defendant admission to infringement, but with claim that he believed erroneously that criminal offense required financial gain.** In *United States v. Dove*, No. 2:07CR00015, 2008 WL 3979467 (W.D. Va. Aug. 25, 2008), the defendant admitted to participating in scheme to produce and distribute infringing files online, but claimed he had not made any money in connection with the scheme and that he erroneously believed that infringement was not criminal in the absence of financial gain. The court permitted a "willful blindness" instruction at trial.

Conversely, other factors may be relevant to finding an absence of "willfulness":

- **Evidence of the defendant's good-faith belief that his conduct was lawful, coupled with rational attempts to comply with the copyright law as understood by the defendant.** *Compare United States v. Moran*, 757 F. Supp. 1046, 1051-53 (D. Neb. 1991) (court in bench trial finding police officer who operated a "mom-and-pop" video rental business not guilty, because he made single copies of lawfully purchased videos and rented the copies only to prevent vandalism of original tapes, and because his activities were "conducted in such a way as not to maximize profits, which one assumes would have been his purpose if he had acted willfully") *with United States v. Sherman*, 576 F.2d 292, 297 (10th Cir. 1978) (affirming conviction of defendants who claimed a good-faith belief that pirated tapes they manufactured and sold were "sound-a-likes," and thus noninfringing). *See also Danjaq, L.L.C. v. Sony Corp.*, 263 F.3d 942, 959 (9th Cir. 2001) (stating that one who has been notified that his conduct constitutes copyright infringement, but who reasonably and in good faith believes the contrary, has not acted willfully) (citing 4 *Nimmer on Copyright* § 14.04).

- **Acting pursuant to legal counsel, even if the advice was erroneous, if the defendant disclosed all relevant circumstances to his attorney and followed the attorney's advice in good faith.** *See* 4 *Nimmer on Copyright* § 14.04[B][3][a]; David M. Nissman, *Proving Federal Crimes* §§ 27.07-.08 (Corpus Juris Publishing 2004).

Possible alternative charges that require lower *mens rea* standards are discussed in Section F. of this Chapter.

3. Infringement of the Copyright

The next element is that the defendant infringed a copyright. *See* 17 U.S.C. § 506(a). "Infringement" refers to the violation of one or more of the exclusive rights granted to a copyright owner at 17 U.S.C. § 106. Infringement is implicitly defined in 17 U.S.C. § 501(a):

> Anyone who violates any of the exclusive rights of the copyright owner as provided by [17 U.S.C. §§ 106-122] or of the author as provided in [17 U.S.C. § 106A(a)], or who imports copies or phonorecords into the United States in violation of [17 U.S.C. § 602], is an infringer of the copyright.

Consequently, infringement may include more than violation of the rights enumerated in § 106 (and also include violations of the rights to exclude imports under § 602, or the rights of certain authors to attribution and integrity defined in § 106A(a)), and at the same time, may not extend to *all* violations of the rights in § 106 (because the rights enumerated in § 106 are "subject to [the limitations of] §§ 107 through 122"). For purposes of criminal enforcement, however, the relevant types of infringement are those enumerated in § 106. (An author's rights to attribution and integrity under § 106A(a) are not enforceable criminally. *See* 18 U.S.C. § 506(f).)

Section 106 of Title 17 sets out the copyright owner's exclusive rights. These rights consist of the rights "to do and to authorize" the following:

- to reproduce a work in copies or phonorecords, § 106(1);
- to prepare derivative works, § 106(2);
- to distribute copies or phonorecords of the work to the public, § 106(3);
- to perform the work publicly (for certain types of works), § 106(4), (6);
- to display a work publicly (for certain types of works), § 106(5).

Sections 107 through 122 limit these rights, the most notable limitations for criminal enforcement purposes are the public's right to make "fair use" of a work without authorization, the first sale doctrine, limitations on rental of software and musical sound recordings, and exceptions for installing and backing up software, all of which are discussed in detail in Section C. of this Chapter.

Felony penalties apply only to infringement of the reproduction or distribution rights. *See* 17 U.S.C. §§ 506(a), 106(1), (3). Specifically, felony penalties apply only if the infringement involved either "reproduction or distribution" of a minimum number and value of works, *see* 17 U.S.C. § 506(a)(1)(A) and 18 U.S.C. § 2319(b)(1); 17 U.S.C. § 506(a)(1)(B) and 18 U.S.C. § 2319(c)(1), or if the infringement involved "distribution of a work being prepared for commercial distribution," by making it available on a publicly-accessible computer network. *See* 17 U.S.C. § 506(a)(1)(C); 18 U.S.C. § 2319(d)(1). See also Section B.4.c. of this Chapter.

Misdemeanor penalties apply to infringement by reproduction or distribution that meet a lower numeric and monetary threshold—one or more copies of one or more copyrighted works, having a total retail value of more than $1,000. *See* 17 U.S.C. § 506(a)(1)(B), 18 U.S.C. § 2319(c)(3). Misdemeanor penalties also cover willful infringement of *any* of the exclusive rights under § 106, if committed for commercial advantage or private financial gain. See 17 U.S.C. § 506(a)(1)(A), 18 U.S.C. § 2319(b)(3), and the discussion in Section B.4. of this Chapter.

Criminal prosecutions have historically focused on reproduction and distribution because these have generally been the most serious infringements, and these infringements incur the most significant penalties under the current criminal law. However, willful infringement of other exclusive rights may also be sufficiently serious to warrant criminal prosecution, particularly as advances in technology lead greater use of technologies that implicate other exclusive rights, such as the use of Internet "streaming" to disseminate copyrighted material (both legitimately and illegimately). Where appropriate, the Department can and should investigate and prosecute copyright misdemeanors for profit-motivated infringements of other rights, such as public performance, public display, or derivative work.

a. Infringement by Reproduction or Distribution

Felony penalties are provided for willful infringement committed "by the reproduction or distribution" of ten or more copies (or phonorecords) of one or more copyrighted works, with a total retail value of $2,500 or more. There are actually two separate combinations of statutory provisions that provide felony penalties for this type of conduct.

Infringement committed with or without the purpose of commercial advantage or private financial gain can fall under 17 U.S.C. § 506(a)(1)(B) if

the willful infringement was committed "by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1000." For these offenses, 18 U.S.C. § 2319(c)(1) provides felony penalties "if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of $2,500 or more." The statutory maximum penalty is 3 years' imprisonment, 6 for repeat offenders. *See* § 2319(c).

Infringement committed for commercial advantage or private financial gain can also fall under 17 U.S.C. § 506(a)(1)(A), which is a felony if the offense "consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500." 18 U.S.C. § 2319(b)(1). The statutory maximum penalty is 5 years' imprisonment, or 10 for repeat offenders.

There is a slight variation in language between the two provisions that set the $2,500 felony threshold: 18 U.S.C. § 2319(c)(1) requires a total retail value of "$2,500 or more," whereas § 2319(b)(1) requires "more than $2,500." It is unclear whether this variation was intentional.

In addition to the felony penalties discussed in the prior paragraphs, there are also felony penalties in 17 U.S.C. § 506(a)(1)(C) for distribution over a computer network accessible by the public. See Section B.3.b. of this Chapter.

The reproduction and distribution rights are set forth in 17 U.S.C. § 106(1) (exclusive right "to reproduce the copyrighted work in copies or phonorecords") and § 106(3) (exclusive right "to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending").

- **Definition of Copies and Phonorecords**

The term "copies" is often used to refer generically to any material object in which a copyrighted work has been fixed. However, the Copyright Act reserves the term "copies" only for works other than sound recordings. "Copies" are defined as "material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." 17 U.S.C. § 101. "Phonorecords" are what we think of as copies of sound recordings, and are defined as "material objects

in which sounds, other than those accompanying a motion picture or other audiovisual work, are fixed by any method now known or later developed, and from which the sounds can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." *Id*. Thus, examples of a "phonorecord" would include an audio tape or CD, or an MP3 file. Examples of "copies" would include a book, a painting, a piece of sheet music, or a sculpture. A software program on disc or in a file on a computer, or a movie on DVD or videotape, would also be "copies," even though these objects might also include an audio sound track.

Somewhat confusingly, the terms "copy" and "phonorecord" can also refer to the *original* object in which the copyrighted work was fixed, such as a handwritten manuscript, or original studio tapes for a sound recording.

- **"Stealing"**

Infringement is often referred to as a form of theft. For example, 18 U.S.C. § 2319 is located in a chapter of the criminal code entitled, "Stolen Property." Yet infringement is distinct from common-law theft, and requires no showing that the defendant "stole" or deprived another person of a physical copy of a work. Making additional copies of a book, movie, or other work may constitute infringement, even if the defendant obtained his original source for additional copies lawfully. Likewise, although publicly distributing copies that were stolen from the copyright owner could constitute infringement, *cf. United States v. Chalupnik*, 514 F.3d 748 (8th Cir. 2008) (discussing defendant's criminal copyright conviction for distribution of lawfully-produced CDs taken from post office without authorization), it is not always necessary to show that copies were "stolen" in order to show infringing distribution.

i. Reproduction

Reproduction encompasses a wide array of conduct, ranging from a novelist's plagiarizing substantial portions of someone else's book or a musician's sampling several notes from a previously-recorded song, to using a computer to "rip" an audio track into MP3 format or making a bit-for-bit copy of a movie on DVD. In most criminal cases, infringing reproduction involves the production of exact, or nearly-exact, duplicates through digital means, as with computer programs, e-books, music or movies copied onto digital media (e.g., CDs, DVDs, hard drives). Copying need not be so blatant, literal, or complete to qualify as infringement, but criminal cases rarely involve defendants who have copied only a small portion of a copyrighted work. Disputes over whether

songs sound too similar, or whether a movie screenplay copies dialogue or characters from an earlier screenplay, are generally best left to civil lawsuits. Nevertheless, some cases of less-than-wholesale, verbatim copying of an entire work may warrant criminal prosecution.

- **Proof of Infringement by Reproduction**

The best evidence of infringement by reproduction is direct evidence that the defendant copied the victim's work, including, for example eyewitness testimony, emails, or computer logs indicating the copying of particular discs or files. Typically, criminal copyright cases will involve complete, verbatim copying of many copyrighted works, and defendants are generally unlikely to challenge this issue credibly. In fact, defendants often even advertise or otherwise mark the infringing copies as being copies. However, when the copies alleged to be infringing are not essentially identical to the original work, prosecutors may need to prove infringement in greater depth.

Direct evidence of copying is best, but circumstantial evidence may suffice. The circumstantial test is whether (1) the defendant had access to the copyrighted work and (2) that defendant's work is "substantially" or "probatively" similar to the copyrighted material. *See Taylor Corp. v. Four Seasons Greetings, LLC*, 403 F.3d 958 (8th Cir. 2005); *Dam Things from Denmark v. Russ Berrie & Co.,* 290 F.3d 548, 562 (3d Cir. 2002); *Kepner-Tregoe, Inc. v. Leadership Software, Inc.*, 12 F.3d 527, 532 (5th Cir. 1994).

The test of "substantial" or "probative similarity" is whether, considering the two works as a whole, and including both the copyrightable elements and the uncopyrightable ones (such as basic ideas or public-domain expressions that are not eligible for copyright), a reasonable person would conclude that the defendant had actually copied the work from the original. *See Positive Black Talk Inc. v. Cash Money Records, Inc.*, 394 F.3d 357, 370 n.9 (5th Cir. 2004), *abrogated on other grounds by Reed Elsevier, Inc. v. Muchnick*, 130 S.Ct. 1237 (2010); *McCulloch v. Albert E. Price, Inc.*, 823 F.2d 316, 318-19 (9th Cir. 1987), *disagreed with on other grounds*, *Fogerty v. Fantasy, Inc.*, 510 U.S. 517 (1994); *Atari, Inc. v. North American Philips Consumer Elec. Corp*., 672 F.2d 607, 614 (7th Cir. 1982). This standard focuses on the works' similarities rather than their differences. *Cf. United States v. Kim*, 307 Fed. Appx. 324 (11th Cir. 2009) (holding comparison of similarities in district court not erroneous, and rejecting defendant's arguments on appeal that emphasized several differences between infringing copies and originals). Thus, "[i]t is enough that substantial

parts [of a copyrighted work] were lifted; no plagiarist can excuse the wrong by showing how much of his work he did not pirate." *United States v. O'Reilly*, 794 F.2d 613, 615 (11th Cir. 1986) (affirming conviction for infringement of copyright in video games where approximately 70% of defendant's code was identical to copyrighted original) (quoting *Sheldon v. Metro-Goldwyn Pictures Corp.*, 81 F.2d 49, 56 (2d Cir. 1936) (L. Hand, J.)).

Note that this test is designed to determine whether *copying* occurred, not necessarily whether that copying constituted *infringement*. If the court determines that actual copying has occurred, only then does it assess whether the copying was substantial enough to constitute infringement. Unfortunately, many courts also refer to this test as one of "substantial similarity," which can lead to confusion. *See*, *e.g.*, *Sid & Marty Krofft Television Prods., Inc. v. McDonald's Corp.*, 562 F.2d 1157, 1164-65 (9th Cir. 1977) (referring to the test of whether copying occurred as an "extrinsic" test of substantial similarity, while calling the test of whether infringement occurred, i.e., whether copyrightable elements were copied, an "intrinsic" test of substantial similarity). To avoid this confusion, many courts prefer to use the term "probative" similarities to show "actual copying," and "substantial similarity" to show "actionable copying." *See Positive Black Talk Inc.*, 394 F.3d at 370; *Dam Things from Denmark*, 290 F.3d at 562 & n. 19.

If the copyrighted work and the defendant's work are "strikingly similar," the first element of access may be presumed (at least in civil copyright cases), especially when the copyrighted work was widely available. *See, e.g.*, *Playboy Enters. v. Frena*, 839 F. Supp. 1552, 1556 (M.D. Fla. 1993) (holding proof of access unnecessary when defendant made "essentially exact" copies of copyrighted photos that appeared in nationally-circulated magazine); *Bright Tunes Music Corp. v. Harrisongs Music, Ltd.,* 420 F. Supp. 177 (S.D.N.Y 1976) (access may be presumed when a copyrighted work is widely available)

In practice, the government demonstrates "substantial" or "probative" similarity, as well as infringement, by comparing the suspect copy side-by-side against an authentic original. Although ideally, this comparison can be performed against the original maintained on file at the Register of Copyrights (if available), it is not absolutely necessary—an authenticated duplicate of the original work will suffice. *See O'Reilly*, 794 F.2d at 615; *United States v. Shabazz*, 724 F.2d 1536, 1539 (11th Cir. 1984). Victims may assist the government with these comparisons. See Chapter X of this Manual; *cf. United States v. Sherman*,

576 F.2d 292, 295 (10th Cir. 1978) (mentioning that suspected pirated tapes were checked by record company before search warrant issued).

- **Statutory Exceptions for Reproduction**

As noted above, copyright owners' rights are limited in 17 U.S.C. §§ 107-122. Several of these provisions particularly limit the reproduction right, including § 107 ("fair use"), § 108 (certain copying by libraries and archives), § 115 (compulsory license for making phonorecords of musical works), and § 117 (certain limited copying of software). See Section C. of this Chapter.

ii. Distribution

Section 106(3) of Title 17 grants copyright owners the exclusive right "to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending." 17 U.S.C. § 106(3). The distribution right is implicated by a wide variety of conduct, such as the sale of books at a bookstore, used CDs at a garage sale, and pirated DVDs at a flea market; the lending of books by a library; and transferring pirated software to other users on the Internet without financial motive. Distribution also includes other transfers of ownership such as gifts or barter. *Ford Motor Co. v. Summit Motor Prods., Inc.*, 930 F.2d 277, 299 (3d Cir. 1991) (citing H.R. Rep. No. 94-1476, at 62, *reprinted in* 1976 U.S.C.C.A.N. 5659, 5675-76 *and* 17 U.S.C.A. § 106 (West 1997) (historical note)).

Although it is occasionally argued that "distribution" requires the transfer of a *physical, tangible* copy and therefore that transmission of electronic files online cannot infringe the distribution right, it is clear that the right to "distribute" copies of works includes the right to distribute them in electronic form, and can be infringed by electronic transfers of copies. *See*, *e.g.*, 17 U.S.C. § 506(a)(1)(C) (defining offense for "distribution" of pre-release works on a public computer network); *N.Y. Times Co. v. Tasini*, 533 U.S. 483, 498 (2001) (discussing distribution of articles through online databases).

- **"To the Public"**

Although often referred to merely as "distribution," the right protected by § 106 is, more specifically, the right to distribute copies or phonorecords of the work "*to the public*." 17 U.S.C. § 106(3) (emphasis added). Giving a single copy of a work to a family member or close friend may not qualify as a "distribution" for copyright purposes, although courts have found under some circumstances that even the giving of a single copy to one person may constitute "distribution

to the public." *Ford Motor Co.*, 930 F.2d at 299-300. *But see Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008) (concluding that cable television service's "remote DVR" system, wherein a copy of a program was transmitted to an individual customer after being recorded at customer's request, did not constitute distribution "to the public" for purposes of § 106).

The Copyright Act does not expressly define "distribution" or "public," except through definitions of other closely-related terms. The term "publication" is defined in § 101, and is often used interchangeably with distribution, and several courts have noted that the two terms are "for all practical purposes synonymous" in the context of a first publication. *Ford Motor Co.*, 930 F.2d at 299; *see also Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 552 (1985); *Agee v. Paramount Comm'ns, Inc.*, 59 F.3d 317, 325 (2d Cir. 1995); *Elektra Entm't Group, Inc. v. Barker*, 551 F. Supp. 2d 234, 240-43 (S.D.N.Y. 2008); 2 *Nimmer on Copyright* § 8.11[A], at 8-148 to 8-149. Some courts have held, however, that "[i]t is not clear that the terms 'publication' and 'distribution' are synonymous outside the context of first publication." *Atlantic Recording Corp. v. Howell*, 554 F. Supp. 2d 976, 984 (D. Ariz. 2008) ("the definition of publication in § 101 of the statute makes clear that all distributions to the public are publications, but it does not state that all publications are distributions"); *London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153, 168-69 (D. Mass. 2008) ("even a cursory examination of the statute suggests that the terms are not synonymous.... By the plain meaning of the statute, all 'distributions ... to the public' are publications. But not all publications are distributions to the public").

Section 101 also defines the term "publicly," with respect to performances and display of works, as referring to "place[s] open to the public or any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered."

For cases discussing distribution "to the public" in several contexts, such as computer networks and subscription based services, see Section B.3.c.ii. of this Chapter.

- **Importation**

Infringing articles are often manufactured overseas and then shipped into the United States for distribution. Under 17 U.S.C. § 602, importation of infringing copies into the United States without permission of the copyright owner generally constitutes "an infringement of the exclusive right to distribute

copies or phonorecords under section 106." Although § 602 specifies that unauthorized importation is a violation of the distribution right (thus providing a basis for criminal prosecution under § 506), and states further than unauthorized importation is "actionable under section 501," § 602 does not expressly mention criminal actions under § 506. To date, no reported case has prohibited prosecutors from bringing an action pursuant to § 506 as a result of a violation of 17 U.S.C. § 602. However, in cases involving importation, prosecutors alternatively should consider charging the defendant with bringing goods into the United States by false statements, 18 U.S.C. § 542, or with smuggling goods, 18 U.S.C. § 545.

- **Making Works Available on the Internet Without Transferring Them**

In the context of peer-to-peer ("P2P") file-sharing networks, placing materials on a website, or other similar methods by which copyrighted materials might be downloaded online, a question may arise as to whether a defendant who merely makes copyrighted material available to others to download copies has infringed the distribution right, in the absence of any evidence of an actual transfer of infringing works. If a P2P user has made movies, music, or software available to the public by placing them in a shared area of his networked desktop computer, but his computer contained no records of whether or how many times these files were downloaded by others, and there is no other evidence that the copyrighted works the defendant "made available" were actually transferred to another computer (or indeed, if there is evidence that no such transfers actually occurred, despite the defendant's having made the files available), has the defendant nevertheless infringed the distribution right in the works (setting aside for the moment the question of whether the defendant may have infringed the reproduction right by copying the files in the first place, or whether the defendant may be infringing the public performance or display rights in the work)? There is no clear answer, however, as described more below, courts will likely require proof of at least some form of dissemination to have occurred in order to find a defendant guilty of a criminal violation of the distribution right.

Several civil cases addressing online infringement suggest that the distribution right is infringed at the point when the defendant makes a file publicly available. *See A&M Records v. Napster, Inc.*, 239 F.3d 1004, 1014 (9th Cir. 2001) (noting that "Napster users who upload file names to the search index for others to copy violate plaintiffs' distribution rights. Napster users who

download files containing copyrighted music violate plaintiffs' reproduction rights."); *Motown Record Co., LP v. DePietro*, No. 04-CV-2246, 2007 WL 576284, at *3 n.38 (E.D. Pa. Feb. 16, 2007) ("While neither the United States Supreme Court nor the Third Circuit Court of Appeals has confirmed a copyright holder's exclusive right to make the work available, the Court is convinced that 17 U.S.C. § 106 encompasses such a right ...."); *Elektra Entm't Group, Inc. v. Doe*, No. 5:08-CV-115-FL, 2008 WL 5111885 (E.D.N.C., Sept. 26, 2008); *Warner Bros. Records, Inc. v. Doe*, No. 5:08-CV-116-FL, 2008 WL 5111884 (E.D.N.C., Sept. 26, 2008); *see also Playboy Enters. v. Chuckleberry Publ'g, Inc.*, 939 F. Supp. 1032, 1039 (S.D.N.Y. 1996) (uploading content on Internet and inviting users to download it violates exclusive publication right); *Playboy Enters. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503, 513 (N.D. Ohio 1997) ("Defendants disseminated unlawful copies of PEI photographs to the public by adopting a policy in which RNE employees moved those copies to the generally available files instead of discarding them."); *Getaped.Com, Inc. v. Cangemi*, 188 F. Supp. 2d 398, 402 (S.D.N.Y. 2002) (holding that copyrighted material was published when it was placed on website and available for viewing or downloading).

A case frequently cited for the proposition that "making available" violates the distribution right is *Hotaling v. Church of Jesus Christ of Latter-Day Saints*, 118 F.3d 199 (4th Cir. 1997). At issue in *Hotaling* was whether a church library open to the public had distributed the plaintiff's work by having it in its collection and listing it in its card catalog, even though no evidence indicated that the work had actually been borrowed or viewed by library patrons. The defendant argued that holding the work in its collection constituted a mere offer to distribute, at most, not an actual distribution. The court sided with the plaintiffs:

> When a public library adds a work to its collection, lists the work in its index or catalog system, and makes the work available to the borrowing or browsing public, it has completed all the steps necessary for distribution to the public. At that point, members of the public can visit the library and use the work. Were this not to be considered distribution within the meaning of § 106(3), a copyright holder would be prejudiced by a library that does not keep records of public use, and the library would unjustly profit by its own omission.

Id. at 203. At least one court considering *Hotaling* focused on the opinion's concern with potential prejudice from a library that kept no records, and suggested that the same logic might apply in online cases where no records are kept. In *Arista Records, Inc. v. MP3Board, Inc.*, No. 00CIV.4660(SHS), 2002 WL 1997918, at *4 (S.D.N.Y. Aug. 29, 2002) (citing *Hotaling*, 118 F.3d at 204), the court considered that "a copyright holder may not be required to prove particular instances of use by the public when the proof is impossible to produce because the infringer has not kept records of public use," but declined to find that an actual distribution had occurred based on the facts before it (in which investigators for the record industry had determined only that hyperlinks on the defendant's website pointed to infringing audio files). *Id*.

Many other courts have sought to resolve peer-to-peer lawsuits while avoiding resolution of "making available" arguments. *See*, *e.g.*, *Arista Records LLC v. Gruebel*, 453 F. Supp. 2d 961, 969 (N.D. Tex. 2006) ("[M]aking copyrighted works available to others may constitute infringement by distribution in certain circumstances."); *Maverick Recording Co. v. Goldshteyn*, No. 05-CV-4523, 2006 WL 2166870, at *3 (E.D.N.Y. July 31, 2006) (Plaintiff's "'making available' argument need not be decided here."); *Fonovisa, Inc. v. Alvarez*, No. 1:06-CV-011, 2006 WL 5865272, at *2 (N.D. Tex. July 24, 2006) ("This Court is not making a determination as to whether 'making works available' violates the right of distribution.").

The Copyright Office states that U.S. copyright law includes a "making available" right that covers making files available on the Internet. *See* U.S. Copyright Office, DMCA Section 104 Report, Vol. 1, at 93-95 (August 2001) *available at* http://www.copyright.gov/reports/studies/dmca/sec-104-report-vol-1.pdf. This, however, does not necessarily resolve the issue for criminal cases because the Copyright Office characterizes this "making available right" as resulting from a combination of the distribution, reproduction, public display, and public performance rights. *Id*. at 94. Because the felony copyright provisions apply only to infringement of the distribution and reproduction rights, it is unclear whether "making available" (as the Copyright Office interprets it) can support a felony charge.

More recently, however, most courts confronting the "making available" issue in civil cases involving either peer-to-peer filesharing or other online contexts have determined that infringing "distribution" requires the dissemination of an actual copy, or have at least expressed some skepticism that mere "making available" is sufficient to constitute infringement. *See Perfect 10,*

Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1162 (9th Cir. 2007) (distribution requires actual dissemination of a copy); *Capitol Records, Inc. v. Thomas*, 579 F. Supp. 2d 1210, 1218-19 (D. Minn. 2008) (plain meaning of "distribution" requires actual dissemination and does not include merely making available); *Elektra v. Barker*, *supra*, 551 F. Supp. 2d 234 (S.D.N.Y. 2008) (mere allegation of "making available" not sufficient to plead infringement, although noting that an offer to distribute copies for further distribution to others would be sufficient); *London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153, 168-69 (D. Mass. 2008) ("Merely because the defendant has 'completed all the steps necessary for distribution' does not necessarily mean that a distribution has actually occurred."); *see also Atlantic Recording Corp. v. Brennan*, 534 F. Supp. 2d 278, 282 (D. Conn. Feb 13, 2008) (denying plaintiffs' entry of default against defendant, in part, by finding that defendant may have a meritorious defense against plaintiffs' "problematic" make available argument); *Atlantic Recording Corp. v. Howell*, 554 F. Supp. 2d 976, 981 (D. Ariz. 2008).

A number of other federal courts have held that distribution requires that an infringing copy actually be disseminated. *See Obolensky v. G.P. Putnam's Sons*, 628 F. Supp. 1552, 1555 (S.D.N.Y. 1986) (directing verdict for defendants after jury trial because the right to distribute is not violated "where the defendant offers to sell copyrighted materials but does not consummate a sale" or "where there is copying, but no sale of the material copied"), *aff'd*, 795 F.2d 1005 (2d Cir. 1986); *accord Paramount Pictures Corp. v. Labus*, No. 89-C-797-C, 1990 WL 120642, at *4 (W.D. Wis. Mar. 23, 1990); *National Car Rental Sys., Inc. v. Computer Assocs. Int'l, Inc.*, 991 F.2d 426, 430 (8th Cir. 1993) (holding that distribution requires the transfer of an actual copy, as § 106(3) grants the copyright owner the "exclusive right publicly to sell, give away, rent or lend any *material embodiment* of his work") (quoting 2 *Nimmer on Copyright* § 8.11[A], at 8-123 (emphasis added by *National Car Rental*)); *cf. In re: Aimster Copyright Litig.*, 252 F. Supp. 2d 634, 643 (N.D. Ill. 2002) (noting, without analysis, that a peer-to-peer user "with copyrighted music files on his hard drive available for download can [once another user searches for and locates a file on the first user's computer] thereafter become an unauthorized distributor of that copyrighted music as soon as another Aimster user initiates a transfer of that file."), *aff'd*, 334 F.3d 693 (7th Cir. 2003). The leading copyright treatise also supports this view. *See* 2 *Nimmer on Copyright* § 8.11[A], at 8-124.1 ("Infringement of [the right to distribute] requires an actual dissemination of either copies or phonorecords.").

Only one criminal decision has addressed this question, albeit in the context of deciding whether state court charges were preempted by federal copyright law: "Posting software on a bulletin board where others can access and download it is distribution ... which is governed by the [federal] copyright laws." *State v. Perry*, 697 N.E.2d 624, 628 (Ohio 1998).

In 2005, Congress created a new offense for infringement of "pre-release" content (*see infra*, Sec. B.3.c.) that unfortunately does not appear to have resolved the "making available" issue. Section 506(a)(1)(C) makes it a felony to willfully infringe "by the distribution of [a pre-release work] by making it available on a computer network accessible to members of the public ...." To date, few courts have had the opportunity to address what "making available" means in the context of § 506(a)(1)(C). Thus far, the only published opinion to discuss the issue is *In re Napster, Inc. Copyright Litig.*, 377 F. Supp. 2d 796 (N.D. Cal. 2005). In that opinion, the court considered the plaintiffs' motion for summary judgment on their claims that Napster had directly infringed the plaintiffs' copyrights by creating and maintaining an indexing system that allowed users to upload and download infringing music files. *Id.* at 802. The key question was "whether the Copyright Act requires proof of the actual dissemination of a copy or phonorecord in order to establish the unlawful distribution of a copyrighted work in violation of 17 U.S.C. § 106(3)." *Id*. The court concluded that distribution did not include the mere offer to distribute a copyrighted work, given the plain meaning and legislative history of the terms "distribution" and "publication." *See id.* at 803-04. The court concluded that "to the extent that *Hotaling* suggests that a mere offer to distribute a copyrighted work gives rise to liability under section 106(3), that view is contrary to the weight of [the] above-cited authorities." *Id.* at 803 (citations omitted). Finally, the court rejected the argument that the "making available" language in the new offense at 17 U.S.C. § 506(a)(1)(C), discussed in Section B.3.c.ii. of this Chapter, evinced Congress's intent that "making available" was a type of distribution, concluding that § 506(a)(1)(C) made willful copyright infringement and "making available" two separate elements. *Napster*, 377 F. Supp. 2d at 805.

Given this backdrop, courts deciding criminal cases are likely to require proof of actual dissemination of copies, as opposed to evidence that the defendant merely "made [infringing works] available," if only to satisfy the rule of lenity. *See United States v. Wiltberger*, 18 U.S. 76, 95 (1820); *Dowling v. United States*, 473 U.S. 207, 213, 228-29 (1985) (applying rule of lenity to

construe stolen property laws narrowly in light of copyright law). Moreover, courts might consider Congress's choice not to punish attempts in § 506 as further evidence that distribution, in criminal cases, requires an actual transfer of an infringing copy to the public.

Some of the civil cases in which proof of actual dissemination has not been required suggest an alternative rule—that where, due to the defendant's actions, no records exist of actual transfers, the court may infer or presume that actual dissemination took place. *See Hotaling*, 118 F.3d 199; *Arista Records*, 2002 WL 1997918. That rule, however, might not be adopted in criminal cases, in which infringing distribution must be proven beyond a reasonable doubt.

As a practical matter, evidence of actual infringing transfers strengthens other aspects of the case. Even if a theory of distribution without dissemination were accepted by the court, a jury might nevertheless reject it—either in sympathy toward a defendant who ostensibly copied nothing, or by concluding that the defendant could not have understood that his conduct constituted infringement sufficiently to establish willful behavior. See the discussion of willfulness in Section B.2. of this Chapter.

When proving that the defendant actually distributed infringing copies, distributions to law enforcement officers or to agents working for the victim should suffice, as a matter of law. *See Capitol Records Capitol Records, Inc. v. Thomas*, 579 F. Supp. 2d 1210, 1216 (D. Minn. 2008) (distribution of copies to investigator can form the basis for civil claim of infringing distribution right); *Atlantic Recording Corp. v. Howell*, 554 F. Supp. 2d 976, 985 (D. Ariz. 2008) (holding that 12 infringing copies downloaded by copyright owner's investigators constituted unauthorized distributions); *Gamma Audio & Video, Inc. v. Ean-Chea*, No. 91-11615-Z, 1992 WL 168186 at *3 n.5 (D. Mass. July 3, 1992), *rev'd in part on other grounds*, 11 F.3d 1106 (1st Cir. 1993); *Paramount Pictures*, 1990 WL 120642 at *5. *But see London-Sire Records, Inc.*, 542 F. Supp. 2d at 166 (stating in dicta that copyright holder's investigator's "own downloads are not themselves copyright infringements because it is acting as an agent of the copyright holder, and copyright holders cannot infringe their own rights"). In some cases, a defendant may have evinced a clear intent to share copyrighted content online in an infringing manner, but sufficient evidence of specific instances of dissemination may be difficult or impossible to obtain. Prosecutors should consider whether the conduct at issue may be appropriately characterized as an infringement of the reproduction right. Further, although attempts to violate § 506 are not criminalized, in appropriate cases a charge

of conspiracy to violate § 506 may be an alternative option. The government need not prove an actual dissemination if the charge is conspiracy to violate the criminal copyright laws by means of distribution. That is, because conspiracy is an inchoate crime, the government need not prove that the underlying crime of distribution was completed.

- **First Sale**

Under 17 U.S.C. § 109, it is not an infringement for the owner of a lawfully-acquired copy or phonorecord of a work to sell or otherwise dispose of that particular copy. This exception is often referred to as the "first-sale" doctrine. For example, a person who purchases a book at a bookstore may later resell the book at a yard sale or donate it to a library, without the copyright-holder's permission. Although first sale is treated as a defense in civil cases, some criminal copyright cases have held that the government must plead and prove the absence of a first sale as an element of the offense. See Section C.4.c. of this Chapter.

b. Infringement of at Least 10 Copies of 1 or More Copyrighted Works With a Total Retail Value Exceeding $2,500 Within a 180-Day Period

i. Generally

The final element for felony offenses under 17 U.S.C. § 506(a)(1)(A) and (B) is that the infringement consisted of the "reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500." 18 U.S.C. § 2319(b)(1); *see also* 18 U.S.C. § 2319(c)(1) (alternative felony provision, applying when value is "$2,500 or more"). For definition of "copies" and "phonorecords," see Section B.3.a. of this Chapter (discussing 17 U.S.C. § 101).

Congress reserved felony penalties for those who copy or distribute a minimum of 10 copies to exclude from felony prosecution low-level infringement such as "children making copies for friends as well as other incidental copying of copyrighted works having a relatively low retail value," and also to avoid having the criminal provisions used as a "tool of harassment" in business disputes involving issues such as reverse engineering or the scope of licenses. H.R. Rep. No. 102-997, at 6 (1992), *reprinted in* 1992 U.S.C.C.A.N. 3569, 3574.

Congress used the phrase "of one or more copyrighted works" as a way "to permit aggregation of different works of authorship to meet the required number of copies and retail value." *Id*. Congress gave as an example a defendant who reproduces 5 copies of a copyrighted word-processing computer program with a retail value of $1,300 and 5 copies of a copyrighted spreadsheet computer program also with a retail value of $1,300. Aggregating these reproductions "would satisfy the requirement of reproducing 10 copies having a retail value of at least $2,500, if done within a 180-day period." *Id.*

ii. Definition of "Retail Value" as an Element of the Offense

Congress left the term "retail value" "deliberately undefined since in most cases it will represent the price at which the work is sold through normal retail channels." *Id.*

Based on both the plain meaning of the statutory text and the legislative history of the 1992 Copyright Felony Act, the term "retail value" as used in 17 U.S.C. § 506 and 18 U.S.C. § 2319 refers to the retail value of the infringed item, i.e., the original or genuine item that was infringed, in the market in which it is sold. By contrast, for sentencing purposes, the Sentencing Guidelines defines "retail value" to include either the value of the "infringed item" (the authentic item) or the "infringing item"(the "street" price of a pirated or counterfeit copy) to compute the sentencing offense level, depending on the circumstances of the crime. See the discussion of U.S.S.G. § 2B5.3 cmt. n.2(C) in Section C.1.c.iii. of Chapter VIII of this Manual.

For purposes of proving the dollar value element of criminal infringement under 17 U.S.C. § 506(a)(1) and 18 U.S.C. § 2319(b) or (c), "retail value" means the retail price of a legitimate or genuine copy of the item infringed at the time of the defendant's infringement. *See United States v. Armstead*, 524 F.3d 442, 443 (4th Cir. 2008) (holding that retail value can be "determined by taking the highest of the 'face value,' 'par value,' or 'market value' of copies of the copyrighted material in a retail context"). Calculating a work's retail value can be more complicated when the work has been published in multiple versions—which often occurs with computer software. In civil cases involving infringement of a new version of a software program that had not yet been registered with the Copyright Office, where earlier versions had been registered, some courts have allowed damages only to the extent that the infringed material consists of material from the earlier, registered versions. *See, e.g.*, *Montgomery v. Noga*, 168 F.3d 1282, 1292 (11th Cir. 1999); *Well-Made Toy Mfg. Corp. v.*

Goffa Int'l Corp., 210 F. Supp. 2d 147, 158 (E.D.N.Y. 2002); 2 *Nimmer on Copyright* § 7.16[B][2]. *But see Montgomery*, 168 F.3d at 1294-95 (upholding jury instruction that permitted the jury to calculate the plaintiff's actual damages by considering the market value of newer, unregistered version).

Although the issue of multiple versions presents more significant challenges in the civil context, where registration of the copyright in a particular work is a prerequisite to filing a lawsuit for infringement of that work, the existence of multiple versions can substantially affect the "retail value" of a work for purposes of criminal prosecution as well. For example, where the most recent version of a business software program ("Program 2.0") is being sold through legitimate retail outlets for $200, while legitimate copies of an older version ("Program 1.0") are still being sold, albeit for the lower retail price of $100, a defendant who pirated 20 copies of the new version would be subject to felony penalties (20 copies at $200 each, totaling $4,000), while a defendant who reproduced 20 pirated copies of the older version would only meet the threshold for a misdemeanor (20 X $100= $2,000). In considering whether and how to charge criminal copyright infringement, prosecutors will want to make sure to assess charges based on the specific version of a copyrighted work that was infringed, and if possible, to obtain retail pricing information on the specific version infringed during the relevant period of the defendant's conduct.

iii. Retail Value for Pre-release Works

Prosecutors may choose to include pre-release works in charges brought under 17 U.S.C. § 506(a)(1)(A), (B) and 18 U.S.C. § 2319(b), (c), where, for example, the defendant engaged in criminal infringement of both pre-release and non-pre-release works, or where other elements of the "pre-release" offense may be difficult to prove. Determining the "retail value" of a pre-release work can be challenging because such works, by definition, are not yet sold on the legitimate market, and thus their legitimate retail value may not yet be set. Congress acknowledged the problem and offered several solutions:

> At the same time, the Committee recognizes that copyrighted works are frequently infringed before a retail value has been established, and that in some cases, copyrighted works are not marketed through normal retail channels. Examples include motion pictures [*sic*] prints distributed only for theatrical release, and beta-test versions of computer programs. *In such cases, the courts may look to the suggested retail price, the wholesale*

price, the replacement cost of the item, or financial injury caused to the copyright owner.

H.R. Rep. No. 102-997, at 6-7 (1992) (emphasis added), *reprinted in* 1992 U.S.C.C.A.N. 3569, 3574-75. If the infringed item has no retail value, the important consideration is the harm to the copyright owner, rather than the (presumably smaller value of) profits to the infringer. *See id.* at 6; 138 Cong. Rec. 34,371 (1992) (statement of Sen. Hatch).

Although the Family Entertainment and Copyright Act ("FECA") created a new felony offense to address Internet piracy of "work[s] being prepared for commercial distribution," the Act does not specify a particular method for determining the "retail value" of such works. *See* Pub. L. No. 109-9 § 103, 119 Stat 218, 220-21 (2005) (codified at 17 U.S.C. § 506(a)(1)(C)). (One possible reason: the "pre-release" offense created by the FECA requires no minimum number or value of infringing copies, in contrast to the 10-copy, $2500 thresholds in previously-existing copyright felonies. *Compare* 17 U.S.C. § 506(a)(1)(C) with 17 U.S.C. § 506(a)(1)(A), (B) and 18 U.S.C. § 2319. The FECA "pre-release" offense is discussed in more detail in Section B.3.c., below.)

In cases where infringement of pre-release works form the basis of a § 506(a)(1)(A) or (B) charge, requiring proof of a minimum "total retail value," prosecutors should consider the alternative methods for valuation discussed in the legislative history above. Also instructive is the approach taken by the U.S. Sentencing Commission in formulating Sentencing Guidelines amendments to address the FECA "pre-release" offense. Those guidelines specify that pre-release works should be valued, for sentencing purposes, at the anticipated retail value of legitimate works upon their legitimate commercial release. *See* U.S.S.G. § 2B5.3 cmt. n.2(A)(vi) (amended Oct. 24, 2005). (The Guidelines also include a 2-level enhancement for offenses involving pre-release works. *See id.* § 2B5.3(b)(2); and Section C.1.c.iii. of Chapter VIII of this Manual.) Where the basis for a § 506(a)(1)(A) or (B) charge consists of a mixture of pre-release and non-pre-release works, the safest course for prosecutors may be to ensure that the $2500 threshold can be demonstrated based on the value of non-pre-release works alone.

iv. $2,500 Threshold

To charge a criminal copyright violation as a felony in cases not involving a "pre-release" offense, the government must prove that the total retail value of the infringing copies exceeded $2,500. This threshold has one minor

complication: the felony threshold is "more than $2,500" when the defendant acted with a profit motive, 18 U.S.C. § 2319(b)(1), but only "$2,500 or more" when the defendant acted without a profit motive, 18 U.S.C. § 2319(c)(1). To be safe, each felony indictment should charge a value greater than $2,500.

v. Within 180 Days

These technical requirements are sometimes difficult to prove. For example, if a defendant operated a video store that rented only pirated videos, but kept no records that describe who did what and at what time, it might be difficult to prove that the defendant himself reproduced or distributed the videos, or that he did so within a particular 180-day period. If faced with such a case, the government may wish to consider alternative charges—such as conspiracy to commit felony criminal copyright infringement; misdemeanor copyright infringement (which reduces the number of copies to 1 and the retail value threshold to $1,000; see Section B.5. of this Chapter); 18 U.S.C. § 2318 (counterfeit or illicit labels, documentation, or packaging for copyrighted works); or 18 U.S.C. § 2320 (trafficking in goods, services, labels, documentation, or packaging with counterfeit marks)—that have no numerical or monetary thresholds. Section 2320 also has the advantage of punishing attempts, which can be proved when the government lacks records of the completed crime

c. Distribution of a Work Being Prepared for Commercial Distribution, by Making it Available on a Publicly-Accessible Computer Network, if the Defendant Knew or Should Have Known the Work Was Intended for Commercial Distribution

In 2005, Congress added an additional felony offense to address the online infringement of pre-release works. *See* Family Entertainment and Copyright Act of 2005 (FECA), Pub. L. No. 109-9 § 103 (codified at 17 U.S.C. § 506(a)(1)(C)). (This provision is part of Title I of FECA, also known as the "Artists Rights and Theft Prevention Act of 2005" or the "ART Act.") Congress enacted this provision to target two phenomena that it deemed particularly harmful to copyright-holders, especially in combination—"pre-release" piracy and Internet piracy (especially peer-to-peer file-sharing). *See, e.g.*, Remarks on Introduction of Bill in Senate, 151 Cong. Rec. S494 (daily ed. Jan. 25, 2005); Judiciary Committee Report, H.R. Rep. No. 109-33(I), at 4 (2005), *reprinted in* 2005 U.S.C.C.A.N. 220, 223. Section 506(a)(1)(C) makes it a felony to willfully infringe "[i] by the distribution of [ii] a work being prepared for commercial distribution, [iii] by making it available on a computer network accessible to

members of the public, [iv] if such person knew or should have known that the work was intended for commercial distribution." 17 U.S.C. § 506(a)(1)(C) (small Roman numerals added for purposes of illustration).

The new offense eliminates the monetary and numeric thresholds for felony copyright infringement if the defendant distributed pre-release works on a computer network.

i. Distribution

The offense defined under 17 U.S.C. § 506(a)(1)(C) applies only to infringement by distribution (as opposed to the copyright felonies in 17 U.S.C. § 506(a)(1)(A),(B) that apply to infringement by distribution or reproduction). For discussion of proving distribution, see Section B.3.a.ii. of this Chapter.

Section 506(a)(1)(C)'s use of the term "making available" does not resolve the issue of whether "distribution" requires an actual dissemination of infringing copies. As of this writing, the only reported case that has discussed this issue specifically in the context of § 506(a)(1)(C), a civil copyright case, stated that "distribution" and "making available on a computer network" are two *separate* elements of the § 506(a)(1)(C) offense. *See In re Napster, Inc. Copyright Litig.*, 377 F. Supp. 2d 796, 805 (N.D. Cal. 2005). The inclusion of "making available" did not, according to this court, redefine distribution to include making available. See Section B.3.a.ii and the following Section of this Chapter.

Regardless of whether "distribution" legally requires actual dissemination of copies, or is interpreted to include merely offers to provide copies, as a practical matter, evidence of actual dissemination of pre-release copies will generally strengthen the government's case, and should be presented if possible.

ii. Making the Work Available on a Computer Network Accessible to Members of the Public

The next element is "making [the work] available on a computer network accessible to members of the public." *See* 17 U.S.C. § 506(a)(1)(C).

Although the statute does not define "computer network" or "accessible to members of the public," the bill was clearly intended to address piracy over the Internet. *See* H.R. Rep. No. 109-33(I), *reprinted in* 2005 U.S.C.C.A.N. 220; 151 Cong. Rec. S499-500 (daily ed. Jan. 25, 2005) (statement of Sen. Cornyn). Clear examples of "making the work available on a computer network

accessible to members of the public" would include posting the work on a website or placing it in a desktop computer's shared file directory so that peer-to-peer users around the world could access and download it.

"[A] computer network accessible to the public" should be read to include large networks available to substantial numbers of people, even if the network is not immediately accessible to all members of the public, such as a university's campus-wide network, a large but proprietary service like AOL, or a password-protected site on the Internet. This would be consistent with the right at issue ("distribution to the public"), and the statutory definition of "publicly" in the context of displays and performances, which refers to "any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered." *See* 17 U.S.C. § 101; *Playboy Enters., Inc. v. Frena*, 839 F. Supp. 1552, 1557 (M.D. Fla. 1993) (holding that displaying infringing photographs over a computer bulletin board to audience limited to paying subscribers constituted display "to the public"); *accord Video Pipeline, Inc. v. Buena Vista Home Entm't, Inc.*, 192 F. Supp. 2d 321, 332 (D.N.J. 2002), *aff'd on other grounds*, 342 F.3d 191 (3d Cir. 2003); *Video Pipeline, Inc. v. Buena Vista Home Entm't, Inc.*, 275 F. Supp. 2d 543, 554 (D.N.J. 2003). See also Section B.3.a.ii. of this Chapter (discussing "to the public"). *But cf. Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1042-43 (N.D. Ill. 1998) (discussing meaning of electronic communications service "to the public" under the Electronic Communications Privacy Act); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002) (same).

iii. Work Being Prepared for Commercial Distribution

The next element of an offense under § 506(a)(1)(C) is that the infringed work must be a "work being prepared for commercial distribution," which is defined as:

> (A) a computer program, a musical work, a motion picture or other audiovisual work, or a sound recording, if, at the time of unauthorized distribution--
>
> (i) the copyright owner has a reasonable expectation of commercial distribution; and
>
> (ii) the copies or phonorecords of the work have not been commercially distributed; or

> (B) a motion picture, if, at the time of unauthorized distribution, the motion picture--
>
> > (i) has been made available for viewing in a motion picture exhibition facility; and
> >
> > (ii) has not been made available in copies for sale to the general public in the United States in a format intended to permit viewing outside a motion picture exhibition facility.

17 U.S.C. § 506(a)(3). Thus, the definition includes only four types of works: software, musical works, audiovisual works such as movies, and sound recordings. Although these categories make up most of the works pirated online, other types that could also be infringed online—such as books, photographs and other works of visual art—are not included.

When Congress created these provisions, it also created a "preregistration" process allowing owners to "preregister" their "works being prepared for commercial distribution" with the Copyright Office. *See* 17 U.S.C. § 408(f); 37 C.F.R. § 202.16 (effective July 2, 2008); Section B.1.c. of this Chapter (discussing preregistration). However, prosecutors should be aware that the scope of the term "works being prepared for commercial distribution" is narrower for purposes of the criminal offense under § 506(a)(1)(C) than the scope that term was given by the Copyright Office in its preregistration regulations. First, the Copyright Office's regulations cover not only movies, music, and software, but also literary works and advertising or marketing photographs. *See* 37 C.F.R. § 202.16. This is broader than the four classes specified by 17 U.S.C. § 506(a)(3), and therefore some works the Copyright Office considers "works being prepared for commercial distribution" may not qualify as "works being prepared for commercial distribution" for purposes of the criminal "pre-release" offense.

Second, the Copyright Office allows for the preregistration of a work that is in the early stages of development: for example, for motion pictures, filming must have commenced, and for a computer program, at least some of the computer code must have been fixed. *See* 37 C.F.R. § 202.16(b)(2). Although these standards may suffice for preregistration with the Copyright Office, prosecutors should exercise caution in evaluating whether to pursue charges based on works that are substantially incomplete. Cases involving a mere fragment of a work or a substantially incomplete work are more likely to

face difficulties in proving copyrightability and infringement, as well as proving "retail value" and perhaps willfulness as well.

Although the pre-release offense and the preregistration process were enacted at the same time, the plain language of 17 U.S.C. § 506(a)(1)(C) does not require that the "work being prepared for commercial distribution" be preregistered before an infringer can be prosecuted. Nor does the legislative history indicate that Congress intended § 506(a)(1)(C) to apply only to "preregistered" works. Therefore, the FECA amendments did not alter the government's power to prosecute infringement that occurs before preregistration or registration of a work. *See also* 17 U.S.C. § 411 (registration only required to commence civil action).

iv. The Defendant Knew or Should Have Known that the Work Was Intended for Commercial Distribution

The next element in § 506(a)(1)(C) concerning the defendant's awareness that the work was "being prepared for commercial distribution," has a lower *mens rea* than the other elements of the offense, which require proof of "willfulness." For this element, the government does not have to prove that a defendant had actual knowledge that the infringed work was a pre-release work, but rather, the government need only show that the defendant "knew or should have known" that the work was "intended for commercial distribution," which is essentially a negligence standard.

4. Additional Element for Enhanced Sentence: Purpose of Commercial Advantage or Private Financial Gain

Proving that the defendant acted "for purposes of commercial advantage or private financial gain" is often either a primary element of an IP crime or a secondary element that can enhance the defendant's maximum sentence. These issues are covered in Sections B. of this Chapter (setting out elements) and C.1.f. (sentencing factors) of Chapter VIII this Manual.

a. History

Before 1997, U.S. law required the government to prove the defendant's intent to seek commercial advantage or private financial gain in every criminal copyright prosecution. In *United States v. LaMacchia*, 871 F. Supp. 535, 539-40 (D. Mass. 1994), the defendant had operated an internet site that invited users to upload and download pirated software. Presumably recognizing, as the

district court later noted, that the defendant could not have been charged with criminal copyright infringement because he had operated his Internet site for trading pirated works without a profit motive, the government instead charged LaMacchia with wire fraud. The court dismissed that charge, suggesting that applying the broad wire fraud statute to copyright infringement could "subvert the carefully calculated penalties" and the "carefully considered approach" Congress had taken in the area of copyright. *Id.* at 539-40 (*quoting Dowling v. United States*, 473 U.S. 207, 225 (1985)).

In direct response to *LaMacchia*, Congress passed the No Electronic Theft ("NET") Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997), which, among other things, closed the *"LaMacchia* loophole" by eliminating "commercial advantage or private financial gain" as an element of felony copyright infringement. statute. *See* 143 Cong. Rec. 24,324 (1997) (remarks of Rep. Coble); H.R. Rep. No. 105-339, at 4-5 (1997). By enacting what was then 17 U.S.C. § 506(a)(2) (renumbered § 506(a)(1)(B) by the Apr. 27, 2005 amendments), Congress created a felony that only requires the government to prove willful infringement above certain monetary and numerical thresholds.

Congress's swift response to *LaMacchia* recognized how the Internet and then new technology had already dramatically changed the way in which copyright infringement was occurring and the resulting harm caused to copyright owners. Now, as then, the Internet allows people to engage in large-scale digital piracy with little expense, time, or complexity. The ease of Internet piracy reduces (and perhaps eliminates) infringers' need for a financial return even as it significantly affects the market for legitimate goods. *See* Committee Report on No Electronic Theft Act, H.R. Rep. No. 105-339, at 4-5 (1997). Willful infringers can act out of a variety of motives unrelated to profit—including a rejection of the copyright laws, anti-corporate sentiments, or bragging rights in the piracy community—yet still cause substantial financial harm. *Id*.

Even though a profit motive is not a necessary element of every copyright offense, it should nonetheless be charged when possible because it increases the defendant's maximum statutory sentence, increases the guideline sentencing range, increases jury appeal, and can help defeat baseless claims of fair use. See Sections C.5. and E.1 of this Chapter, and Section C.1.f. of Chapter VIII of this Manual.

b. Legal Standard

Essentially, a defendant has acted for "commercial advantage or private financial gain" if he sought a profit, financial or otherwise. *Cf.* 4 *Nimmer on Copyright* § 15.01[A][2] (discussing legislative history to copyright statute).

"Financial gain" is broadly defined to include not only a monetary transaction, but also the "receipt, or expectation of receipt, of anything of value, including the receipt of other copyrighted works." 17 U.S.C. § 101. Bartering schemes are included, where people trade infringing copies of a work for other items, including computer time or copies of other works. Congress added this definition of financial gain in the NET Act specifically to address bartering. *See* No Electronic Theft Act (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997); 143 Cong. Rec. 24,421 (1997) (statement of Sen. Hatch); 143 Cong. Rec. 24,326 (1997) (statement of Rep. Goodlatte). For example, federal prosecutors have successfully charged "commercial advantage or private financial gain" in cases where defendants ran a closed piracy network that distributed pirated works in exchange for access to other pirated works. *See, e.g.,* Department of Justice Press Release, *California Man Pleads Guilty for Role in Distributing Pirated Music During Five-year Period* (May 2, 2011), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2011/montejanoPlea.pdf.

Although courts have had few occasions to consider the scope of "commercial advantage," the plain meaning of the term and case-law in other areas suggest that "commercial advantage" includes not only obtaining payment for infringing products, but also using the infringing products to obtain an advantage over a competitor. This is true even if the defendant charged nothing for the infringing copies. *See Herbert v. Shanley Co.*, 242 U.S. 591, 593-94 (1917) (Holmes, J.) (holding that performing a copyrighted musical composition in a restaurant or hotel, even without charging for admission, infringes the copyright owner's exclusive right to perform the work publicly for profit); *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023 (9th Cir. 2001) (holding that "[f]inancial benefit exists where the availability of infringing material acts as a draw for customers," even when the infringing material is offered for free) (internal quotation marks and citation omitted), *aff'g in pertinent part* 114 F. Supp. 2d 896, 921 (N.D. Cal. 2000) (noting that Napster anticipated deriving revenues from users by offering copyrighted music for free); *Twentieth Century Music Corp. v. Aiken*, 356 F. Supp. 271, 275 (W.D. Pa. 1973) (holding that a business that merely plays background music to relax its employees so that they will be

efficient is infringing for profit), *rev'd on other grounds*, 500 F.2d 127 (3d Cir. 1974), *aff'd* 422 U.S. 151, 157 (1975) (assuming that restaurant owner acted for profit); *Associated Music Publishers v. Debs Mem'l Radio Fund*, 141 F.2d 852 (2d Cir. 1944) (holding that a radio station that without permission broadcasts a copyrighted work for free in order to get, maintain, and increase advertising revenue has done so for profit).

Examples of infringement for commercial advantage include an engineering firm's use of pirated drafting software to keep overhead low, a website that offers free pirated software to generate advertising revenue when downloaders visit the site, and a business that gives away counterfeit goods to draw in customers to whom it then sells legitimate services. In these cases, although the infringer may not expect to receive money or other items of value in exchange for the infringing copies, the infringement saves the business the money it would have spent on authorized copies or licenses. The savings allow the infringer to gain a commercial advantage over competitors who use only licensed copies of copyrighted works.

Whether a defendant actually makes a profit is beside the point: what matters is that he intended to profit. *See* 17 U.S.C. § 101 (defining "financial gain" to include "expectation of receipt" of anything of value); *id.* § 506(a)(1)(A) ("for *purposes* of commercial advantage or private financial gain") (emphasis added); 18 U.S.C. § 2319(d)(2) (same); *United States v. Taxe*, 380 F. Supp. 1010, 1018 (C.D. Cal. 1974) ("'Profit' includes the sale or exchange of the infringing work for something of value in the hope of some pecuniary gain. It is irrelevant whether the hope of gain was realized or not."), *aff'd in part and vacated in part on other grounds*, 540 F.2d 961 (9th Cir. 1976); *United States v. Shabazz*, 724 F.2d 1536, 1540 (11th Cir. 1984) (same); *United States v. Moore*, 604 F.2d 1228, 1235 (9th Cir. 1979) (holding that acting "for profit," as required by earlier version of Copyright Act, includes giving infringing work to a prospective buyer to evaluate for free before purchasing); *United States v. Cross*, 816 F.2d 297, 301 (7th Cir. 1987); *Herbert*, 242 U.S. at 595 (Holmes, J.) (holding that under the copyright statute the performance of a copyrighted work at a hotel or restaurant was for profit, even if customers did not pay specifically for the performance, because "[w]hether it pays or not, the purpose of employing it is profit and that is enough").

Prosecutors should generally refrain from alleging that a defendant obtained financial gain by getting free or discounted infringing works solely as a result of copying or downloading works for himself. This benefit is common

to all infringement, and to hold that mere infringement equals private financial gain would convert every infringement case into one for private financial gain and thus erase important distinctions in the civil and criminal copyright statutes. Although there are apparently no reported opinions on this question in criminal copyright cases, a number of courts have followed this reasoning in interpreting a related statute with criminal and civil penalties for using and trafficking in unauthorized satellite and cable television decoders "for purposes of commercial advantage or private financial gain." 47 U.S.C. § 553(b)(2). These courts held that the mere purchase and use of such a device for the defendant's own benefit and that of his family and friends does *not* constitute "gain" within the meaning of that statute. *See*, *e.g.*, *Comcast Cable Commc'ns v. Adubato*, 367 F. Supp. 2d 684, 693 (D.N.J. 2005) (holding that to qualify as commercial advantage or private financial gain, the defendant must have used the device "to further some commercial venture or profited in some way from the device beyond simply sitting by himself or with his family and friends around a television set using the illegal device to watch programs for which payment should have been made"); *American Cablevision of Queens v. McGinn*, 817 F. Supp. 317, 320 (E.D.N.Y. 1993) (holding that "private financial gain" should not be read to encompass defendant's "gain" from receiving broadcasts himself: such an interpretation would render "gain" enhancement superfluous because all violations would result in gain). *But see Charter Commc'ns Entm't I, LLC v. Burdulis*, 367 F. Supp. 2d 16, 32 (D. Mass. 2005) (holding that defendant who violated § 553 to receive unauthorized cable broadcasts did so for purposes of "financial gain" within the statute); *Cablevision Sys. New York City Corp. v. Lokshin*, 980 F. Supp. 107, 114 (E.D.N.Y. 1997) (same).

A profit motive can be proved by circumstantial evidence. *See United States v. Cross*, 816 F.2d 297, 301 (7th Cir. 1987) ("[T]he presence of these seventeen second-generation videocassettes on [the defendant's] business premises may rationally give rise to the inference that they were maintained for commercial advantage or private financial gain.").

5. Misdemeanor Copyright Infringement

To obtain a misdemeanor conviction under 17 U.S.C. § 506(a) and 18 U.S.C. § 2319, the government must demonstrate that:

1. A valid copyright exists;
2. The copyright was infringed by the defendant;

3. The defendant acted willfully; and

4. The infringement was done EITHER

   (a) for purposes of commercial advantage or private financial gain, 17 U.S.C. § 506(a)(1)(A); 18 U.S.C. § 2319(b)(3); OR

   (b) by reproduction or distribution of one or more copyrighted works with a total retail value of more than $1,000 within a 180-day period, 17 U.S.C. § 506(a)(1)(B); 18 U.S.C. § 2319(c)(3).

Although the misdemeanor and felony crimes share some elements—all require proving willful infringement—the need to prove scope or scale is lessened for misdemeanors. In cases without commercial advantage or private financial gain that involve the reproduction or distribution of infringing copies, the threshold number of copies and monetary value for a misdemeanor are lower than those required for a felony under 18 U.S.C. §§ 2319(b)(1) or (c)(1): all that is required is one or more copies, with a total retail value of $1,000 or more. And in cases of for-profit infringement, the misdemeanor has no numerical or monetary prosecutorial thresholds. 18 U.S.C. § 2319(b)(3). Thus, misdemeanor copyright infringement can be charged when a defendant clearly profited or intended to profit, but where the government cannot prove the exact volume or value of the infringement due to a lack of business records or computer logs.

A misdemeanor charge can also apply to willful, for-profit infringement of rights other than reproduction or distribution, such as the performance right or digital audio transmissions. Although the felony penalties are reserved for infringing reproduction and distribution, the misdemeanor provisions apply "in any other case," *see* 18 U.S.C. § 2319(b)(3), such as the infringement of the other rights.

C. Defenses

1. Statute of Limitations: 5 years

The criminal copyright statute has a five-year statute of limitations. 17 U.S.C. § 507(a). The five-year limitations period was first established by the NET Act, Pub. L. No. 105-147 § 2(c), 111 Stat. 2678 (1997), before which the limitations period had been three years (the same as for civil copyright claims). *See* Copyright Act of 1976, Pub. L. No. 94-553, 90 Stat. 2541 (1976).

2. Jurisdiction

United States copyright law generally has no extraterritorial effect. Although many foreign countries protect United States copyrights against infringement in foreign lands, and domestic law similarly protects foreign copyrighted works against infringement within the United States, 17 U.S.C. § 411(a), U.S. law generally "cannot be invoked to secure relief for acts of [copyright] infringement occurring outside the United States." *Palmer v. Braun*, 376 F.3d 1254, 1258 (11th Cir. 2004); *see also Subafilms, Ltd. v. MGM-Pathe Commc'ns*, 24 F.3d 1088, 1091 (9th Cir. 1994) (en banc); *Update Art, Inc. v. Modiin Pub'g, Ltd.*, 843 F.2d 67, 73 (2d Cir. 1988) ("It is well established that copyright laws generally do not have extraterritorial application.").

This means that some copyright cases cannot be brought in the United States, even when the victims are U.S. companies or nationals and the infringed works are copyrighted in the United States. For example, U.S. law does not grant federal courts jurisdiction over a manufacturing plant in southeast Asia that produces pirated DVDs for sale in Europe, if the infringing conduct occurs solely abroad. *See Palmer*, 376 F.3d at 1258.

In addition, in civil copyright cases, most courts hold that a defendant in the United States who authorizes acts of infringing reproduction or distribution that occur outside the country, standing alone, does not violate United States copyright law sufficient to grant United States courts subject-matter jurisdiction. *See Subafilms*, 24 F.3d at 1091; *Armstrong v. Virgin Records, Ltd.*, 91 F. Supp. 2d 628, 634 (S.D.N.Y. 2000) (reviewing cases and concluding that the *Subafilms* position is more widely accepted). *But see Curb v. MCA Records, Inc.*, 898 F. Supp. 586, 593 (M.D. Tenn. 1995); *Expediters Int'l of Washington, Inc. v. Direct Line Cargo Mgmt. Servs., Inc.*, 995 F. Supp. 468, 476 (D.N.J. 1998).

However, these rules do not bar a United States copyright case if an infringing act *does* occur in the United States in whole or in part. *Palmer*, 376 F.3d at 1258; *Sheldon v. Metro-Goldwyn Pictures Corp.*, 106 F.2d 45, 52 (2d Cir. 1939) (holding that court had power over profits made from showing a copied film outside the country because negatives from which the film was printed were made in the United States); *Rundquist v. Vapiano SE,* 798 F. Supp. 2d 102*,* 123-24 (D.D.C. 2011); *P & D Int'l v. Halsey Pub'g Co.*, 672 F. Supp. 1429, 1432-33 (S.D. Fla. 1987) (finding subject-matter jurisdiction over copyright action because complaint alleged that defendant copied U.S.-

copyrighted film in Florida and then showed the film in international waters aboard cruise ship) (citing 3 *Nimmer on Copyright* § 17.02, at 17-5).

Although to date no reported criminal cases have addressed this issue, the cases cited above provide a sound legal basis for prosecuting criminal infringement domestically when at least a part of the defendant's infringing conduct occurred within the United States. Charging a conspiracy also allows for domestic jurisdiction over criminal copyright co-conspirators located outside the United States, if their co-conspirators act inside the country. *See*, *e.g.*, *Ford v. United States*, 273 U.S. 593, 624 (1927) (holding that a conspiracy charge need not rely on extraterritorial principles if its object crime is in the U.S. and a co-conspirator commits an act in the U.S. to further the conspiracy); *United States v. Winter*, 509 F.2d 975, 982 (5th Cir. 1975).

Additionally, at least in the context of capturing and retransmitting broadcast signals so as to infringe a copyright owner's public performance right, there appears to be some disagreement between the courts as to whether it is necessary for a "complete" act of infringement to take place in the United States for the Copyright Act to apply. The Ninth Circuit has taken the position that at least one "complete" act of infringement must take place in the United States. *See Allarcom Pay Television, Ltd. v. Gen. Instrument Corp.*, 69 F.3d 381, 387 (9th Cir. 1995) (holding that the Copyright Act did not apply to broadcasts of copyrighted material from the United States into Canada because the infringement was not completed until the signals were "received and viewed" in Canada). The Second Circuit, however, has strongly rejected that view, holding that an act of infringement need only be partially completed in the United States. *See Nat'l Football League v. PrimeTime 24 Joint Venture*, 98 CIV. 3778 (LMM), 1999 WL 163181, at *3 (S.D.N.Y. Mar. 24, 1999) (Copyright Act applied where defendant's "transmission of the signals captured in the United States is 'a step in the process by which a protected work wends its way to its audience,' although not the only, or the final, step, and an infringement, even though it takes one or more further steps for the work to reach the public"), *aff'd* 211 F.3d 10, 13 (2d Cir. 2000) (according the Ninth Circuit law "little weight largely because it contains no analysis of the Copyright Act."); *see also WGN Cont'l Broadcasting Co. v. United Video, Inc.,* 693 F.2d 622, 624-25 (7th Cir. 1982) (concluding that an intermediate carrier is not immune from copyright liability simply because it does not retransmit a copyrighted signal to the public directly but instead routes the signal to cable systems, which then retransmit to the public). While *Allarcom* has generally

been limited to its specific facts (and has rarely been applied outside of the Ninth Circuit), prosecutors can avoid the issue, where possible, by charging an act of infringement completed within the United States. As discussed above, prosecutors may also avoid the issue by charging a conspiracy.

For more on the lack of extraterritorial application of U.S. copyright law, see I. Trotter Hardy, U.S. Copyright Office, *Project Looking Forward: Sketching the Future of Copyright in a Networked World, Final Report* 132 (1998), *available at* http://www.copyright.gov/reports/thardy.pdf.

3. Venue

Crimes "begun in one district and completed in another, or committed in more than one district, may be inquired of and prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237(a). Few reported cases have directly addressed this issue in criminal copyright prosecutions. *See United States v. Tucker*, 495 F. Supp. 607, 618 (E.D.N.Y. 1980) (holding that although defendant resided outside district, venue was proper for grand jury investigation into defendant's sales of counterfeit sound recordings because "middleman" in defendant's scheme resided, and purchaser was headquartered, in district). Cases addressing venue in analogous cases suggest that venue would be proper in any district where reproduction or distribution occurred, or through which pirated works were shipped. *Cf. United States v. DeFreitas*, 92 F. Supp. 2d 272, 276-77 (S.D.N.Y. 2000) (holding in criminal trademark case involving importation and distribution of counterfeit "Beanie Babies" that offense was a continuing offense and thus venue was proper in any district where the offense was begun, continued, or completed, i.e., where products entered the U.S., were shipped, or sold); *United States v. Rosa*, 17 F.3d 1531, 1541 (2d Cir. 1994) (holding that in conspiracy to transport stolen goods, venue was proper where the agreement was entered into, or where any overt act in furtherance of the conspiracy was committed).

4. The First Sale Doctrine—17 U.S.C. § 109

a. Operation of the Doctrine

A common defense to a claim of infringement of the distribution right is the "first sale" doctrine, codified at 17 U.S.C. § 109, which provides that "[n]otwithstanding the provisions of section 106(3), the owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to

sell or otherwise dispose of the possession of that copy or phonorecord." In other words, once a copyright-holder sells or gives a specific copy to another person, the copyright-holder generally cannot control how that particular copy is subsequently sold or transferred. *See United States v. Moore*, 604 F.2d 1228, 1232 (9th Cir. 1979); *see also* 2 *Nimmer on Copyright* § 8.12[B] (discussing first sale); 4 *Nimmer on Copyright* § 15.01[A][2] (discussing application of "first sale" in criminal cases). Putting it in terms of the purchaser's rights, the first purchaser and any subsequent purchaser of that specific copy may further distribute or dispose of that particular copy without the copyright-holder's permission.

The first sale doctrine does *not* grant the purchaser or anyone else the right to make additional copies of the copy he owns. Making unauthorized copies of a lawfully-obtained work still violates the law. 4 *Nimmer on Copyright* § 15.01[A][2], at 15-10. Consequently, the first sale doctrine is a defense only against an allegation of infringement by means of distribution.

Moreover, the first sale doctrine may be invoked by a defendant *only* for the distribution of *lawfully-made* copies. If copies were pirated, the first sale doctrine does not apply. *See United States v. Drum*, 733 F.2d 1503, 1507 (11th Cir. 1984) (citing *Moore*, 604 F.2d at 1232); *United States v. Powell*, 701 F.2d 70, 72 (8th Cir. 1983). Additionally, a person may not sell or give away his lawful copy while retaining a backup copy, even a backup copy of software that is authorized by 17 U.S.C. § 117. *See* 17 U.S.C. § 117(a)(2) (requiring destruction of archival copies if continued possession of original copy ceases to be rightful); *see also* 17 U.S.C. § 117(b) (allowing transfer of exact archival copies only with a complete transfer of rights in the original copy). An unlawfully retained backup copy can be an infringing reproduction. See Section C.6. of this Chapter for a discussion of the "archival" exception codified at 17 U.S.C. § 117(a)(2).

The first sale doctrine protects a defendant only if he owned his copy, not if he merely borrowed or rented it. In fact, the first sale doctrine does not "extend to [protect] any person who has acquired possession of the copy or phonorecord from the copyright owner, *by rental, lease, loan, or otherwise, without acquiring ownership of it*." 17 U.S.C. § 109(d) (emphasis added). This is an important distinction for works such as motion picture film reels, which are typically distributed to movie theaters under a lease or similar arrangement, and computer software, which is often distributed subject to a licensing agreement.

It is not always clear, however, whether a commercial transaction of copyrighted works is legally a sale or a licensing agreement, which can make or break a first sale defense. How the parties characterize the transaction to themselves or others may not be controlling as a matter of law. When a computer user "purchases" a copy of software through a retail channel or other means, the licensing agreement may actually assert that the arrangement is not an outright purchase of a copy but merely a license to use the work. Were these licensing agreements the last word on the subject, § 109 would not allow the licensee to resell his software. Yet many courts have recharacterized a software publisher's shrinkwrap licensing agreement as a sale when the publisher distributes its software through retail channels. *See Softman Prods. Co. v. Adobe Sys., Inc.*, 171 F. Supp. 2d 1075 (C.D. Cal. 2001); *Novell, Inc. v. Network Trade Ctr., Inc.*, 25 F. Supp. 2d 1218, 1230 (D. Utah 1997), *vacated in part on other grounds*, 187 F.R.D. 657 (D. Utah 1999); *ProCD, Inc. v. Zeidenberg*, 908 F. Supp. 640 (W.D. Wis. 1996), *rev'd on other grounds*, 86 F.3d 1447 (7th Cir. 1996); *see also Krause v. Titleserv, Inc.*, 402 F.3d 119 (2d Cir. 2005); Mark Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. Cal. L. Rev. 1239, 1244 n.23 (1995) (discussing cases). Other courts have taken the opposite position, however, holding that a copy of software obtained subject to license is not subject to the first sale doctrine or other benefits of "ownership." *See Apple Inc. v. Psystar Corp.* 658 F.3d 1150, 1155-56 (9th Cir. 2011); *Vernor v. Autodesk, Inc.,* 621 F.3d 1102 (9th Cir. 2010), *cert. denied,* 132 S. Ct. 105 (2011); *Adobe Sys., Inc. v. Stargate Software Inc.*, 216 F. Supp. 2d 1051, 1058 (N.D. Cal. 2002); *Adobe Sys. Inc. v. One Stop Micro, Inc.*, 84 F. Supp. 2d 1086, 1089 (N.D. Cal. 2000); *Microsoft Corp. v. Software Wholesale Club, Inc.*, 129 F. Supp. 2d 995, 1002 (S.D. Tex. 2000) (citing *Microsoft Corp. v. Harmony Computers & Elec., Inc.*, 846 F. Supp. 208, 212-14 (E.D.N.Y. 1994)); *see also* Lemley, 68 S. Cal. L. Rev. at 1244 n.23.

Although no reported criminal case to date appears to have addressed the specific issue of whether an unauthorized transfer of a lawfully-obtained copy of software subject to an end-user license agreement can constitute criminal copyright infringement, the question may yet arise in cases involving "repackaged" software, in which some elements of the software package are genuine, while others are copied or altered. *See*, *e.g.*, *Stargate Software Inc.*, 216 F. Supp. 2d at 1058 (rejecting argument that first sale doctrine should apply to academic versions of software repackaged and sold as retail versions). In such cases, prosecutors may wish to consider other charges, such as 18 U.S.C. § 2318 (counterfeit or illicit labels, documentation, or packaging for

copyrighted works). *See United States v. Harrison,* 534 F.3d 1371 (11th Cir. 2008) (holding that the first sale doctrine does not apply to 18 U.S.C. § 2318).

An important question concerning first sale, recently resolved by the Supreme Court, concerns whether it applies to copies produced abroad and later imported into the United States. Federal courts had reached differing conclusions on this issue. *See, e.g., Quality King Distribs., Inc. v. L'anza Research Int'l, Inc.*, 523 U.S. 135, 145 (1998) (first sale doctrine under § 109 permits reimportation and resale of copy originally produced legally in the United States); *Omega S. A. v. Costco Wholesale Corp.*, 541 F. 3d 982, 986 (9th Cir. 2008) (§ 109 permits resale of copies manufactured abroad only if an authorized first sale occurs within the United States), *aff 'd by an equally divided court*, 562 U. S. ___ (2010); *Sebastian Int'l, Inc. v. Consumer Contacts (PTY) Ltd.*, 847 F. 2d 1093, 1098 n.1 (3rd Cir. 1988) (limitation of the first sale doctrine to copies made within the United States "does not fit comfortably within the scheme of the Copyright Act"). In *Kirtsaeng v. John Wiley & Sons, Inc.*, No. 11-697, __ U.S. __ (Mar. 19, 2013), the Supreme Court held that the first sale provision of § 109 applies to copies "lawfully made" outside the United States, thus permitting purchasers of copies manufactured abroad to import such copies into the U.S. and sell or otherwise distribute them within the U.S. without permission from the copyright owner, so long as the copies were originally produced with the copyright owner's authorization.

b. Affirmative Defense or Part of the Government's Case-in-Chief

Courts disagree as to whether the government must prove absence of "first sale" as part of its case-in-chief in a criminal case. *See* 4 *Nimmer on Copyright* § 15.01[A][2], at 15-8 to 15-9. In civil cases, "first sale" is an affirmative defense. *See* 2 *Nimmer on Copyright* § 8.12[A]; H.R. Rep. No. 94-1476, at 81 (1976) ("It is the intent of the Committee, therefore, that in an action to determine whether a defendant is entitled to the privilege established by section 109(a) and (b), the burden of proving whether a particular copy was lawfully made or acquired should rest on the defendant."), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5695.

The better rule is to apply the civil rule in criminal cases. *See, e.g.*, *United States v. Larracuente*, 952 F.2d 672, 673-74 (2d Cir. 1992); *United States v. Goss*, 803 F.2d 638, 643-44 (11th Cir. 1986); *United States v. Drum*, 733 F.2d 1503, 1507 (11th Cir. 1984). There is no good reason for shifting an affirmative defense in civil cases to an element of the offense in criminal cases,

given that the government must already prove that the defendant engaged in infringement willfully. Yet several cases state the opposite, that in criminal cases the government must negate first sale as an element of the offense. *See, e.g.*, *United States v. Cohen*, 946 F.2d 430, 434 (6th Cir. 1991)*; United States v. Sachs*, 801 F.2d 839, 842 (6th Cir. 1986); *United States v. Powell*, 701 F.2d 70, 72-73 (8th Cir. 1983); *United States v. Moore*, 604 F.2d 1228, 1232-33 (9th Cir. 1979); *United States v. Wise*, 550 F.2d 1180, 1191-92 (9th Cir. 1977); *United States v. Atherton*, 561 F.2d 747, 749 (9th Cir. 1977); *United States v. Drebin*, 557 F.2d 1316, 1326 (9th Cir. 1977); *United States v. Wells*, 176 F. Supp. 630, 633 (S.D. Tex. 1959).

c. Disproving First Sale at Trial

The easiest way to negate the first sale doctrine is to introduce evidence of reproduction of unauthorized copies. Two types of circumstantial proof typically suffice. First, the government can introduce evidence that the defendant obtained his copies illegitimately. *See Moore*, 604 F.2d at 1232 (holding that government may establish absence of first sale by circumstantial evidence, as well as by tracing distribution); *United States v. Whetzel*, 589 F.2d 707, 711-12 (D.C. Cir. 1978) (holding that tapes' illicit origin was shown by labels on tapes listing a manufacturer with a non-existent address, tapes' low price, and the circumstances of their sale), *abrogated on other grounds*, *Dowling v. United States*, 473 U.S. 207 (1985). Factors indicating that copies were obtained illicitly include the sale of copies at a price far below the legitimate market value, the distribution of copies of inferior quality, the existence of copies with identical serial numbers, and the presence of false information on the copies, such as a false address for the manufacturer, fictitious labels, or sales under suspicious circumstances. *See, e.g.*, *Drum*, 733 F.2d at 1507 (rebuttal of first sale defense included direct and circumstantial evidence concerning fictitious labels, low prices, and clandestine sale); *Whetzel*, 589 F.2d at 712 (sale of copies of tapes from the back of a van in a parking lot).

Second, the government can introduce evidence that the copyright holder never sold copies of the work at all, which shows that the defendant could not have obtained ownership of legitimate copies. *See United States v. Sachs*, 801 F.2d 839 (6th Cir. 1986) (holding that government negated the first sale doctrine with respect to movie videotapes with evidence that the original movies had never been sold legitimately in same format); *United States v. Drebin*, 557 F.2d 1316 (9th Cir. 1977) (holding that government proved the absence of first sale through evidence that copyrighted movies had never been

sold or transferred and that licenses transferring limited rights for distribution and exhibition of the films for a limited time were not "sales" for purposes of the first sale doctrine). *But see United States v. Atherton*, 561 F.2d 747 (9th Cir. 1977) (holding that government failed to prove the absence of first sale because, although the copyright owner never "sold" film copies, it permitted a major television network to permanently retain copies and sold scrap film to salvage company for consideration, all of which fell within the definition of first sale and could have been the defendant's source).

The government need not account for the distribution of *every* copy of a work. *See, e.g.*, *Moore*, 604 F.2d at 1232 ("[T]he Government can prove the absence of a first sale by showing that the [copy] in question was unauthorized, and it can establish this proof ... by circumstantial evidence from which a jury could conclude beyond a reasonable doubt that the recording was never authorized and therefore never the subject of a first sale."); *see also Sachs*, 801 F.2d at 843 (holding that the government need not trace every single copy to its origins, because "[t]he other recognized method of satisfying [the first sale] doctrine is for the government to ... show that the copies in question have illegitimate origins"); *Drum*, 733 F.2d at 1507 ("The government may prove the absence of a first sale by direct evidence of the source of the pirated recordings or by circumstantial evidence that the recording was never authorized.") (citations omitted); *Whetzel*, 589 F.2d at 711 ("It was not required to disprove every conceivable scenario in which appellant would be innocent of infringement.").

d. Special Rules for Rental, Lease, and Lending

Although the first sale doctrine extends to almost all types of copyrighted works, it has some limitations with respect to some types of sound recordings and computer programs, which generally may be resold or given away but cannot be rented, leased, or loaned without the copyright-owner's permission. *See* 17 U.S.C. § 109(a), (b)(1)-(2) (describing exception and the types of computer programs that do not qualify for the exception). *But see* § 109(b)(2)(A) (providing that this does not apply to the rental, lease, or loan of a phonorecord for nonprofit purposes by a nonprofit library or educational institution). Regardless, the unauthorized (and thus infringing) rental or lending of sound recordings and computer programs is not subject to criminal penalties. *See* § 109(b)(4).

Although unauthorized rental or leasing of certain types of works is not directly subject to criminal sanctions, businesses that advertise or engage in

this type of conduct might still be subject to criminal copyright infringement penalties. For example, assume that a business rents CDs containing music and tells its customers to "burn it and return it," i.e., to make a copy before bringing it back. Would the above rules exempt this business from criminal prosecution? On the one hand, the answer appears to be "yes," since 17 U.S.C. § 109(b)(4) states that the unauthorized rental of sound recordings "shall not be a criminal offense." On the other hand, this conduct may extend beyond mere "unauthorized rental" to active solicitation, aiding-and-abetting, or conspiracy to commit criminal copyright infringement. No published case has yet addressed this issue.

5. Fair Use

The fair use doctrine is an affirmative defense to copyright infringement. It allows the unauthorized use of copyrighted material under certain circumstances generally limited to useful or beneficial purposes with minimal impact on the market for the work. Specifically, the fair use doctrine, codified at 17 U.S.C. § 107, allows the unauthorized use of copyrighted works "for purposes such as criticism, comment, news reporting, teaching ..., scholarship, or research" and other, unspecified, purposes and uses.

Fair use is designed to ensure that the rights of authors are balanced with the interest of the public in the free flow of information. *See*, *e.g.*, Pierre Leval, *Toward a Fair Use Standard*, 103 Harv. L. Rev. 1105, 1110 (1990) (commentary by Judge Pierre Leval, United States District Court for the Southern District of New York). Congress has noted that fair use is the most important limitation on the exclusive rights granted copyright owners, H.R. Rep. No. 94-1476, at 65 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5678, and the Supreme Court has characterized fair use as one of copyright law's built-in accommodations to the First Amendment. *See Eldred v. Ashcroft*, 537 U.S. 186, 219-20 (2003).

By design, the fair use doctrine is fluid and applies not according to definite rules, but rather according to a multi-factor balancing test. *See* H.R. Rep. No. 94-1476, at 66 (1976). The statute cites four non-exclusive factors:

> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
>
> (2) the nature of the copyrighted work;

(3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

(4) the effect of the use upon the potential market for or value of the copyrighted work.

17 U.S.C. § 107. Other unspecified factors may be appropriate. It would be difficult to articulate a more determinate set of fair use rules, given the variety of copyrighted works, their uses, and the situations in which they can be used. Consequently, both through case law and statutory codification, fair use has historically been decided on a case-by-case basis looking at the totality of the facts at hand. *See* H.R. Rep. No. 94-1476, at 65-66 (1976). Although the fair use doctrine has developed primarily in civil cases, those cases have precedential weight in criminal cases.

The first factor to consider is the purpose and character of the use. 17 U.S.C. § 107(1). A commercial use is presumptively unfair, whereas for a noncommercial, nonprofit activity, "[t]he contrary presumption is appropriate." *Sony Corp. of Am. v. Universal Studios*, 464 U.S. 417, 449 (1984). Nevertheless, "the mere fact that a use is educational and not for profit does not insulate it from a finding of infringement, any more than the commercial character of a use bars a finding of fairness." *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 584 (1994).

Another consideration relevant to the first factor is whether the use is "transformative" or, in other words, adds something new or different beyond a mere repackaging or restatement of the original: "Although such transformative use is not absolutely necessary for a finding of fair use, the goal of copyright, to promote science and the arts, is generally furthered by the creation of transformative works." *Id.* at 579 (citation omitted); *see also* Leval, 103 Harv. L. Rev. at 1111 ("The use must be productive and must employ the quoted matter in a different manner or for a different purpose from the original. A quotation of copyrighted material that merely repackages or republishes the original is unlikely to pass the test."). If a work is transformative, other factors that normally weigh against finding of fair use, such as the commercial nature of the use, bear less weight. *See Acuff-Rose*, 510 U.S. at 579.

The second factor is the nature of the copyrighted work. *See* 17 U.S.C. § 107(2). "This factor calls for recognition that some works are closer to the core of intended copyright protection than others." *Acuff-Rose*, 510 U.S. at 586. Fair use is more difficult to establish in the use of fictional or purely

creative or fanciful works, as opposed to more factual or historical (yet still copyrightable) works, such as recollections of public figures, or depictions of newsworthy events. *See id.* "The law generally recognizes a greater need to disseminate factual works than works of fiction or fantasy." *Harper & Row, Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 563 (1985).

The third factor is the amount and substantiality of the use "in relation to the copyrighted work as a whole." *See* 17 U.S.C. § 107(3). A defense of fair use is less likely to succeed if the portion of the copyrighted material used is substantial in quantity or importance. *See Harper & Row*, 471 U.S. at 564-66 (holding news magazine's 300-word excerpt of book not to be fair use because quoted sections were key passages). However, a use can be fair even if it copies the entire work. *See Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004) (granting summary judgment to group that had published voting machine manufacturer's entire email archive to publicly expose machines' flaws); *Kelly v. Arriba Soft Corp.*, 336 F.3d 811 (9th Cir. 2003) (holding defendant's copying of entire images to create online searchable database of "thumbnails" was fair use).

The fourth factor is how substantially the use affects the potential market for the copyrighted work or the work's actual value. *See* 17 U.S.C. § 107(4). "[T]o negate fair use one need only show that if the challenged use 'should become widespread, it would adversely affect the *potential* market for the copyrighted work.' This inquiry must take account not only of harm to the original but also of harm to the market for derivative works." *Harper & Row*, 471 U.S. at 568 (citations omitted). The Supreme Court has emphasized the importance of this factor in cases of noncommercial use. *Sony*, 464 U.S. at 451 ("A challenge to a noncommercial use of a copyrighted work requires proof either that the particular use is harmful, or that if it should become widespread, it would adversely affect the potential market for the copyrighted work."). *See Harper & Row*, 471 U.S. at 540-41 (finding that harm to potential market was indicated by fact that magazine cancelled its contract to reprint segment of book after defendant published article quoting extensively from book).

Again, these are non-exclusive factors that may be supplemented as technology and circumstances require. *See* 17 U.S.C. § 107.

a. Unpublished Works

A defendant's use of an unpublished copyrighted work may qualify as a fair use. In 1992, Congress amended 17 U.S.C. § 107 to make explicit that

"[t]he fact that work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors [in § 107(1)-(4)]." Act of Oct. 24, 1992, Pub. L. No. 102-492, 106 Stat. 3145 (1992); *see also* H.R. Rep. No. 102-836, at 7 (1992), *reprinted in* 1992 U.S.C.C.A.N. 2553, 2559 (legislative history underscores that Congress intended there to be no *per se* rule barring the fair use of unpublished works). This was primarily, but not exclusively, out of concern for the needs of biographers, historians, and publishers concerned with court decisions that suggested that they could not use unpublished material of historical interest—such as the unpublished letters and diaries of major authors or public figures—in books or other serious treatments of historical figures and events. *See id.* at 4-9 (citing *Salinger v. Random House, Inc.*, 650 F. Supp. 413 (S.D.N.Y. 1986), *rev'd*, 811 F.2d 90 (2d Cir.), *cert. denied*, 484 U.S. 890 (1987); *New Era Publ'ns Int'l, ApS v. Henry Holt & Co.*, 684 F. Supp. 808 (S.D.N.Y. 1988); *New Era Publ'ns Int'l, ApS v. Henry Holt & Co.*, 695 F. Supp. 1493 (S.D.N.Y. 1988), *aff'd on other grounds*, 873 F.2d 576 (2d Cir. 1989)). Congress heeded this concern and thereafter amended the fair use statute to include the fair use of unpublished works, not limiting it to works of historic value.

b. Fair Use in Criminal Cases

Although the fair use doctrine has been developed mainly through civil cases, it is a defense to a charge of infringement, and thus a legitimate defense in criminal cases. However, fair use rarely comes up in the criminal context, most likely because prosecutors are reluctant to prosecute where fair use is a serious issue. A fair use is not an infringing use, and without an infringement there are no grounds for copyright prosecution. *See* 17 U.S.C. § 107 ("[T]he fair use of a copyrighted work ... is not an infringement of copyright."); 17 U.S.C. § 506(a) (specifying grounds for prosecuting "[a]ny person who *willfully infringes* a copyright") (emphasis added). Moreover, a defendant who believed in good faith that he was engaging in fair use has a complete defense to the *mens rea* element, which requires the government to prove that the defendant infringed willfully. See Section B.2.a. of this Chapter. (As indicated in Section B.2.b., a bad-faith claim of fair use, on the other hand, might help establish willfulness.) Prosecutors are—and generally should be—reluctant to seek charges where the defendant acted "for purposes such as criticism, comment, news reporting, teaching ..., scholarship, or research" or any other use with a beneficial public purpose. *See* 17 U.S.C. § 107.

When the defendant is charged with violating 17 U.S.C. § 506(a)(1)(A)—infringement for purposes of commercial advantage or private financial gain—fair use will ordinarily not be a defense because commercial uses are presumptively unfair. *Sony*, 464 U.S. at 449. On the other hand, some commercial uses, such as commercial parodies of other works, have been found to be fair. *See Acuff-Rose,* 510 U.S. at 594.

Because of the fair use doctrine's concern with noncommercial uses, fair use is more likely to pose a significant defense in criminal cases that do not allege a profit motive, such as large-scale infringement under § 506(a)(1)(B) and certain § 506(a)(1)(C) offenses. However, courts have rejected fair use arguments in civil cases against peer-to-peer file-traders who had no direct commercial motive. *See BMG Music v. Gonzalez*, 430 F.3d 888, 890 (7th Cir. 2005) (finding that a peer-to-peer user who downloaded at least 30 and as many as 1300 songs, and kept them, did "not engage[] in a nonprofit use" for purposes of fair use analysis); *Sony BMG Music Entm't v. Tenenbaum*, 672 F. Supp. 2d 217, 227-28 (D. Mass. 2009) (granting plaintiff's motion for summary judgment as to fair use defense, despite finding that defendant's acts of downloading and distributing 30 copyrighted songs did not constitute "commercial" use, where defendant's use "was not accompanied by any public benefit or transformative purpose that would trigger the core concerns of the doctrine").

That said, there is a wide gulf between the typical criminal copyright case and the typical case in which fair use is a legitimate defense. In most criminal cases, the defendant does not even arguably act "for purposes such as criticism, comment, news reporting, teaching ..., scholarship, or research." *See* 17 U.S.C. § 107. Furthermore, many criminal prosecutions involve the wholesale piracy of commercially popular works, in which a fair use defense would be undercut by the fair use factors concerning "the amount and substantiality of the portion used in relation to the copyrighted work as a whole," and "the effect of the use upon the potential market for or value of the copyrighted work." § 107(3), (4). The works are generally copied in their entirety, and the wide availability of the free, pirated copies (which suffer no degradation in quality in digital form) can have a drastic effect on the potential market for legitimate works. A strong showing on these factors will help overcome the presumption that noncommercial use is fair.

6. "Archival Exception" for Computer Software—17 U.S.C. § 117

Section 117 of Title 17 provides a limited exception to the blanket rule against copying, by allowing one who owns a copy of a computer program to copy the program as necessary to use the program or do machine maintenance or repair, and as an archival backup, subject to certain limitations. Specifically, § 117(a) provides that "it is not an infringement [of copyright] for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program" under two circumstances. The first is if the making of the copy or adaptation is "an essential step in the utilization of the computer program in conjunction with a machine, and that [the copy] is used in no other manner." 17 U.S.C. § 117(a)(1). Essentially, this allows the lawful owner of a piece of software to install it on his machine, even if doing so requires copying the program from a CD-ROM to the hard drive or loading it from the hard drive into RAM, both of which are considered reproduction under copyright law. *See Micro-Sparc, Inc., v. Amtype Corp.*, 592 F. Supp. 33 (D. Mass. 1984) (holding that purchasers of programs sold in printed form do not infringe copyright by typing code into computer in order to use the programs); *Summit Tech., Inc. v. High-Line Med. Instruments Co.*, 922 F. Supp. 299 (C.D. Cal. 1996) (holding that owners of ophthamological laser system did not infringe copyright by turning on system to use it, causing copy of manufacturer's data table to be loaded into system RAM); *cf. MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993) (holding that loading of copyrighted software into RAM by service company constitutes reproduction).

The second circumstance in which § 117 allows copying is if the copy is "for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful." 17 U.S.C. § 117(a)(2). This provision allows one who owns a piece of software to make a backup copy for safekeeping, but requires him to destroy his backup copies if he sells or otherwise transfers his original copy or if his ownership otherwise ceases to be rightful.

A third subsection of § 117 provides it is not an infringement for a machine's owner or lessee to make or authorize the making of a copy of a computer program if the copy is made solely as a result of the activation of a machine containing a lawful copy of the software, and the copy is used solely to repair or maintain the machine, and is destroyed immediately thereafter. 17 U.S.C. § 117(c); *see also Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc.*, 431 F.3d 1374, 1375 (Fed. Cir. 2005).

Section 117's exceptions benefit the "owner of a copy of a computer program" or, in the case of machine repair and maintenance, "the owner or lessee of a machine." 17 U.S.C. § 117(a), (c). However, because most computer software is distributed subject to a license, rather than a conventional outright sale, the question arises (in much the same way as it does in the context of "first sale" under § 109) whether § 117 allows copying by a person who has legally obtained a copy of a computer program, but licenses rather than "owns" the software. See the discussion of first sale in Section C.4. of this Chapter. As with the analogous first sale question, courts are split on the issue. *Compare Krause v. Titleserv, Inc.*, 402 F.3d 119 (2d Cir. 2005) (holding client to be an "owner," for § 117(a) purposes, of copies of computer programs written for it by consultant despite lack of formal title in copies, because it had paid consultant to develop programs for its sole benefit, copies were stored on client's server, and client had right to use or discard copies as it saw fit) *with CMAX/ Cleveland, Inc. v. UCR, Inc.*, 804 F. Supp. 337 (M.D. Ga. 1992) (holding that licensee of copyrighted computer software system and its employees were not entitled to computer program owner's defense to copyright-holder's copyright infringement action, because the licensee and employees never "owned" copy of the program, and there was evidence that the licensee was going to market its program); *cf. ISC-Bunker Ramo Corp. v. Altech, Inc.*, 765 F. Supp. 1310 (N.D. Ill. 1990) (holding defendant not entitled to § 117 exception because it acquired copy from competitor and possession was unauthorized).

Some sellers of pirated software display a disclaimer or other notice claiming that their distribution of unauthorized copies is somehow permitted under 17 U.S.C. § 117. Such claims are baseless. Although there are no reported criminal cases addressing this defense, courts have interpreted § 117 narrowly. *See*, *e.g., Micro-Sparc, Inc.,* 592 F. Supp. at 35 (while § 117 allowed owners of written copy of source code to type it in to their own computers, it did not permit third-party business to type in source code and sell it on diskette). Moreover, the fact that a defendant was sufficiently aware of copyright issues to make a frivolous or bad-faith claim of compliance with § 117 may help establish willfulness. *Cf. United States v. Gardner*, 860 F.2d 1391, 1396 (7th Cir. 1988) (holding "Notice of Warning" by seller of "black boxes" for receiving unauthorized cable television, disclaiming liability for any illegal uses, "establish[es] that he was well aware that his actions were unlawful"); *United States v. Knox*, 32 F.3d 733, 754 (3d Cir. 1994) (rejecting argument that disclaimers in brochure stating that child pornography videos were legal disproved the *mens rea* element and because "[i]f anything, the need to profess legality should have alerted

[defendant] to the films' dubious legality"); *Rice v. Paladin Enters., Inc.*, 128 F.3d 233, 254 (4th Cir. 1997) (holding that jury could find the "For academic study only!" disclaimer in promotional sales catalog for "Hit Man" book "to be transparent sarcasm designed to intrigue and entice").

D. Emerging and Special Issues

Most of the special issues in criminal copyright law concerning registration, Internet piracy, and pre-release piracy have been addressed throughout this chapter. Additional emerging areas involving streaming and linking sites are briefly highlighted below. Prosecutors who encounter emerging and special issues involving streaming, linking sites or others not addressed in this chapter should contact CCIPS at (202) 514-1026 for further advice or to suggest them for an update to be published in the electronic edition of this Manual.

1. Internet Streaming

The past decade has seen a rapid rise in the use of Internet "streaming" technology as a means to disseminate content online. "Streaming" generally refers to the delivery of digital media content in real time, so that it may be watched, listened to, or played contemporaneously with the transfer of the media data to a recipient's device. Popular streaming media sites and services currently include YouTube, Hulu, Vimeo, Pandora, and Spotify. Netflix and Amazon, for instance, offer online streaming of movies in addition to offering copies of movies for sale or rental, and (in the case of Amazon) offering downloads of music files for a fee. There are also a large and growing number of Internet sites that offer infringing content via streaming, many of which derive substantial revenues through advertising or user subscription fees.

In contrast to a "download" model, in which a recipient receives a complete and permanent copy of a media file, when media content is delivered solely for streaming, the recipient will generally not retain a complete or permanent copy of the media file on the receiving device (although pieces of the media file being received may be buffered or stored temporarily as part of the streaming process). Streaming is also comparatively resource intensive, as playing media files to many different users in real time, without pauses or gaps, requires powerful servers and significant amounts of Internet bandwidth. Widespread use of streaming has become an increasingly viable option to disseminate media content both legitimately and illegitimately as costs for data storage processing power and bandwidth have fallen significantly.

Although currently unsettled, existing criminal copyright laws (as of this writing) are not ideally suited to address serious cases of infringing streaming. The penalty provisions in 18 U.S.C. §2319 were drafted in an era when the vast majority of online infringement involved the creation and transfer of complete and permanent electronic copies. As a result, existing criminal copyright law provides felony penalties only for infringements that involve the "reproduction" or "distribution" of a minimum number of copies above a threshold value. To the extent that streaming of copyrighted works does not involve creating or transferring complete or permanent copies of a work, it is generally viewed as implicating copyright's "public performance" and "public display" rights in a work, rather than the "reproduction" or "distribution" rights. *See*, *e.g.*, *United States v. Am. Soc'y of Composers, Authors, and Publishers*, 485 F. Supp. 2d 438, 442-47 (S.D.N.Y. 2007) (distinguishing between distribution and performance of digital music); 3 William F. Patry on Copyright § 8:23 (2012). Accordingly, an illegal streaming site that willfully infringes copyrighted works by streaming may not violate the reproduction or distribution rights to a sufficient degree to be eligible for felony copyright penalties.

As of this writing, there have been several legislative proposals to amend criminal copyright penalties to address significant cases involving Internet streaming. *See, e.g.*, Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations at 10 (March 2011), *available at* http://www.whitehouse.gov/sites/default/files/ip_white_paper.pdf; Commercial Felony Streaming Act, S. 978 112th Cong. (2011). In general, these proposals would expand copyright felony penalties to apply to infringements of the "public performance" or "public display" rights under certain circumstances.

Setting aside possible legislative changes, prosecutors have other options to pursue significant cases involving Internet streaming. For example, even though a site may be primarily engaged in Internet streaming, the site may also be engaged in related conduct that involves felony reproduction or distribution. Some sites that offer streaming of infringing content also allow users to download complete copies, typically for an additional fee. Assembling a pirate streaming site also requires the infringing content to be copied onto the site's servers. This copying, if sufficient to meet the numeric and monetary thresholds (and other elements) of 18 U.S.C. § 2319, may form a sufficient basis for a felony charge.

Existing law also provides misdemeanor penalties for willful infringements involving any of the exclusive rights protected by copyright (not just reproduction and distribution) when committed for purposes of commercial advantage or private financial gain. *See* 17 U.S.C. § 506(a)(1)(A); 18 U.S.C. 2319(b)(3). Because streaming is relatively resource intensive, major infringing streaming sites are generally supported by advertising or subscriber fees, and, therefore, one option for pursuing a site willfully engaged in infringing streaming is to charge one or more misdemeanors.

2. Cyberlockers and Linking Sites

Although remote storage of data files has long been a staple use of the internet and other online services (*see, e.g.*, Electronic Communications Privacy Act (ECPA) of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (creating definition, at 18 U.S.C. § 2711(2), of "remote computing service")), the past several years have witnessed a rapid rise in the use of a new generation of online file storage services, referred to generically by such terms as "cloud storage" or "web storage" services, "webhards," or "cyberlockers." A wide range of sites and services fall into this category, including Amazon's Cloud Drive, Apple's iCloud, Microsoft's SkyDrive, Google Drive, Dropbox, Rapidshare, MediaFire, and Filesonic. The specific features, intended uses, and target markets for these services vary widely; some are designed and marketed primarily for data backup or for access to personal files while traveling, while some are focused more on facilitating transfers of large data files to others. Many provide substantial amounts of storage for free. The capability of cyberlocker services to disseminate large media files has led to their use in large scale piracy of movies, music, software, and other copyrighted works.

Although the use of cyberlockers to infringe copyright is a relatively recent trend, the same principles apply to cyberlockers as to other types of online infringement. Individual users of cyberlockers who make use of cyberlockers to reproduce, distribute, or otherwise infringe copyright willfully may be prosecuted criminally, provided the other elements of the criminal copyright statute (e.g., minimum numeric and monetary thresholds; commercial advantage or private financial gain; online distribution of pre-release works) are met. Operators of cyberlockers may also be subject to prosecution for criminal copyright infringement where they willfully distribute or disseminate infringing content, or under theories of aiding and abetting or conspiracy to commit criminal copyright infringement. *See* 18 U.S.C. §§ 2, 371.

To the extent that cyberlockers are used to distribute large media files to a group or to the public, they function much like popular user-generated content ("UGC") sites like YouTube or Vimeo. However, a common feature that generally distinguishes cyberlockers from UGC sites is that cyberlockers are generally not designed to be searchable by outside users or the web-crawlers used by search engines to index publicly-available content on the Internet. On many cyberlocker sites, the only way to access a particular file is to know the specific URL or address where the file is located (e.g., a complex and difficult-to-guess address such as, "http://www.cyberlocker.com/xyzcvbRT1908973"). Partly as a result, an ecosystem of "linking sites" has developed that compile and categorize links to media files located on cyberlocker sites (as well as BitTorrent or other links to P2P networks), enabling users to search for and locate particular files, including pirated media content. Many of these linking sites are supported by advertising, and some may also receive affiliate commissions in exchange for driving traffic to a cyberlocker or other content-hosting site.

The fact that a "pure" linking site does not host infringing content itself may present additional challenges to criminal prosecution. Most courts that have addressed the issue in civil cases have held that merely providing links to infringing content does not violate the distribution right or otherwise constitute direct copyright infringement (although such conduct may still result in secondary liability under a theory of contributory or vicarious infringement). *See*, *e.g.*, *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (2007); *Online Policy Grp. v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1202 n.12 (N.D. Cal. 2004) ("[H]yperlinking per se does not constitute direct copyright infringement because there is no copying."); *Arista Records, Inc. v. MP3Board, Inc.*, No. 00 CIV 4660 (SHS), 2002 WL 1997918, at *4 (S.D.N.Y. Aug. 29, 2002) (linking to content does not violate the distribution right or constitute direct infringement). The extent to which merely linking to infringing content hosted by other sites may constitute *criminal* copyright infringement under 17 U.S.C. § 506 has not been conclusively resolved by the courts. Regardless of whether linking itself amounts to a substantive violation of § 506, however, defendants who facilitate infringement by others by providing links to infringing material online may nevertheless by prosecuted under theories of aiding and abetting (18 U.S.C. § 2) or conspiracy (18 U.S.C. § 371), provided that the other requisite elements of criminal infringement (e.g., willfulness, numeric and monetary thresholds, online distribution of pre-release work) can be shown.

E. Penalties

1. Statutory Penalties

Whereas the substantive crime of copyright infringement is set forth at 17 U.S.C. § 506(a), the penalties for that conduct are set forth at 18 U.S.C. § 2319. *See* 17 U.S.C. § 506(a) ("Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18.").

A misdemeanor carries a sentence of up to one year of imprisonment and a $100,000 fine or twice the monetary gain or loss. *See* 18 U.S.C. §§ 2319(b)(3),(c)(3), 3571(b)(5), (d). For the crimes that qualify as misdemeanors, see Section B.5. of this Chapter.

A first-time felony conviction under 17 U.S.C. § 506(a)(1)(A) carries a five-year maximum sentence of imprisonment and a fine up to $250,000 or twice the monetary gain or loss; repeat offenders face the same fine and ten years of imprisonment. 18 U.S.C. §§ 2319(b)(1),(2), 3571(b)(3),(d) (specifying fines for Title 18 offenses where the fine is otherwise unspecified).

A first-time felony conviction under 17 U.S.C. § 506(a)(1)(B) carries a three-year maximum sentence of imprisonment and a fine up to $250,000 or twice the monetary gain or loss; repeat offenders face the same fine and six years' imprisonment. 18 U.S.C. §§ 2319(c)(1),(2), 3571(b)(3),(d).

A first-time felony conviction under 17 U.S.C. § 506(a)(1)(C) carries a three-year maximum sentence—five years if the offense was committed for purposes of commercial advantage or private financial gain—and a fine of $250,000 or twice the monetary gain or loss; repeat offenders face the same fine and twice the jail time (six or ten years, depending on whether the offense was committed for purposes of profit). 18 U.S.C. §§ 2319(d), 3571(b)(3), (d).

2. Sentencing Guidelines

All sentencing guideline issues concerning the criminal copyright statute are covered in Chapter VIII of this Manual.

F. Other Charges to Consider

Prosecutors may wish to consider the following crimes in addition to or in lieu of criminal copyright charges.

- **Aiding-and-abetting, inducement, and conspiracy**

Prosecutors may, for strategic reasons, wish to bring accessory charges, such as aiding-and-abetting or inducement, 18 U.S.C. § 2, or conspiracy, 18 U.S.C. § 371. *See, e.g.*, *United States v. Sachs*, 801 F.2d 839 (6th Cir. 1986) (affirming conviction for aiding-and-abetting and conspiring to infringe in motion picture copyright infringement case); *United States v. Allan*, No. 95-CR-578-01, 2001 WL 1152925 (E.D. Pa. Sept. 18, 2001) (denying motion to vacate sentence on defendant's convictions for, among other things, copyright infringement, aiding-and-abetting, and conspiracy).

Aiding-and-abetting and inducement of criminal copyright infringement under 18 U.S.C. § 2 are similar to the "inducement" theory of secondary liability the Supreme Court recently endorsed in *Metro Goldwyn-Mayer Studios, Inc. v. Grokster*, 545 US 913 (2005). Although *Grokster* was a civil case, further decisions in the case on remand, as well as subsequent civil litigation on the same topic, will likely provide further guidance on how an inducement theory may be applied in criminal copyright cases.

- **Trafficking in recordings of live musical performances, 18 U.S.C. § 2319A**

As discussed in Section B.1.a.i. of this Chapter, a work must be fixed in a tangible medium in order to enjoy copyright protection. Thus, live musical performances are not protected by copyright unless they are "fixed" by an audio recording authorized by the performer. However, the law provides copyright-like protections for live musical performances by prohibited unauthorized recordings of such performances, and trafficking in such recordings. *See* 17 U.S.C. § 1101 (providing civil remedies); 18 U.S.C. § 2319A (criminal sanctions). These protections were enacted in 1994 in part to comply with obligations under international copyright treaties that require protection for musical performances. *See* Uruguay Round Agreements Act, Pub. L. No. 103-465, 108 Stat. 4809 (1994). Specifically, 18 U.S.C. § 2319A(a) subjects to criminal sanctions:

> [w]hoever, without the consent of the performer or performers involved, knowingly and for purposes of commercial advantage

> or private financial gain - (1) fixes the sounds or sounds and images of a live musical performance in a copy or phonorecord, or reproduces copies or phonorecords of such a performance from an unauthorized fixation; (2) transmits or otherwise communicates to the public the sounds or sounds and images of a live musical performance; or (3) distributes or offers to distribute, sells or offers to sell, rents or offers to rent, or traffics in any copy or phonorecord fixed as described in paragraph (1), regardless of whether the fixations occurred in the United States.

Although some unauthorized recordings or trade in unauthorized recordings might be prosecuted as infringement of the underlying musical composition performed in the recording, § 2319A specifically targets the making and distribution of these so-called "bootlegged" musical recordings.

Each of § 2319A's three subsections protects a different right of the performing artist. Paragraph (a)(1) prohibits fixing the sounds or images of a live musical performance in a tangible medium. *See* 17 U.S.C. § 101 (defining fixation). *But see United States v. Moghadam*, 175 F.3d 1269, 1274 (11th Cir. 1999) (declining to decide whether a live performance is fixed at the time of performance). Paragraph (a)(2) prohibits transmitting the sounds or images of a live musical performance to the public. This subsection was intended to apply to the unauthorized transmission of bootleg performances through radio or television, and not to the unauthorized reproduction of previously recorded but unreleased performances, i.e., studio out-takes. The latter should be considered for prosecution as criminal copyright infringement or, if labeled, trafficking in counterfeit labels, documentation, or packaging. See Chapter VI of this Manual. Paragraph (a)(3) prohibits distributing to the public or trafficking in any fixed recording of a live musical performance.

Under each subsection, the government must also prove that the defendant acted: (1) without authorization from the performer involved; (2) knowingly; and (3) for purposes of commercial advantage or private financial gain. See Section B.4. of this Chapter for a detailed discussion of the commercial motivation element.

Section 2319A is a five-year felony (ten years for repeat offenders) with a fine of $250,000 or twice the monetary gain or loss, *see* 18 U.S.C. §§ 2319A(a), 3571(b)(3),(d), and is sentenced under the same guideline as are copyright

crimes, U.S.S.G. § 2B5.3. The statute provides for mandatory forfeiture and destruction of all infringing items upon a defendant's conviction. *See* 18 U.S.C. § 2319A(b),(c). Further, a violation of § 2319A is listed in 18 U.S.C. § 1961(1)(B) as a RICO predicate. It was inserted into RICO by the Anticounterfeiting Consumer Protection Act, Pub. L. No. 104-153 § 3, 110 Stat. 1386 (1996).

The constitutionality of 18 U.S.C. § 2319A (and the related civil statute, 17 U.S.C. § 1101) has been challenged several times on the grounds that in the area of copyright Congress may regulate only "writings" and only for "limited times," *see* U.S. Const., art. I, § 8, cl. 8, and that § 2319A (which has no time limit and applies to live performances) exceeds those limits. Although these challenges have occasionally prevailed at the district court level, the constitutionality of the statute has ultimately been upheld upon rehearing or by the Courts of Appeals. *See United States v. Martignon*, 492 F.3d 140 (2d Cir. 2007); *Moghadam*, 175 F.3d at 1274-77; *Kiss Catalog, Ltd. v. Passport Int'l Prods., Inc.*, 405 F. Supp. 2d 1169 (C.D. Cal. 2005).

Many states also criminalize trafficking in bootleg recordings.

- **Unauthorized recording of motion pictures in a motion picture exhibition facility ("Camcording"), 18 U.S.C. § 2319B**

The Family Entertainment and Copyright Act of 2005, Pub. L. No. 109-9, 119 Stat. 218 (enacted April 27, 2005), created a criminal offense that targets "camcording," the use of camcorders and similar devices to record movies playing in public movie theaters. "Camcorded" copies of movies are a significant source of pirated movies, and sales of camcorded copies of movies can be especially harmful to copyright owners, because they typically are created and distributed when the movie is available only in theaters and not on DVD or other formats. H.R. Rep. No. 109-33(I) (2005), *reprinted in* 2005 U.S.C.C.A.N. 220. In addition to the federal camcording offense in § 2319B, most states and the District of Columbia also provide criminal penalties for unauthorized camcording.

The elements of an offense under 18 U.S.C. § 2319B are that the defendant (1) knowingly, and (2) without the authorization of the copyright owner, (3) used or attempted to use an audiovisual recording device, (4) to transmit or make a copy of a motion picture or other audiovisual work protected under Title 17, (5) from a performance of such work in a motion picture exhibition facility. 18 U.S.C. § 2319B(a). The maximum punishment for the offense is three years (six years for repeat offenders). *Id*.

Section 2319B's *mens rea* requirement is lower than the "willfulness" requirement for criminal copyright offenses: a § 2319B defendant need only act "knowingly." Additionally, it is not necessary to show infringement of a copyright. Rather, the government need only show that the defendant was transmitting or copying (or attempting to transmit or copy) a copyrighted motion picture without the copyright owner's permission. Although the defenses to infringement set forth in Title 17 would not apply to a prosecution under 18 U.S.C. § 2319B, the statute's legislative history indicates that Congress intended prosecutors to avoid prosecuting cases that would be deemed "fair use" under copyright law. *See* H.R. Rep. No. 109-33(I), at 4.

An "audiovisual recording device" is defined as a "digital or analog photographic or video camera, or any other technology or device capable of enabling the recording or transmission of a copyrighted motion picture or other audiovisual work, or any part thereof, regardless of whether audiovisual recording is the sole or primary purposes of the device." 18 U.S.C. § 2319B(g)(2). This would appear to apply to camera-phones, PDA phones, and digital cameras (especially those capable of recording video). Congress, however, intended that the offense should not cover incidental uses of these devices in a theater, even though such uses could violate other statutes (such as the copyright laws). *See* H.R. Rep. No. 109-33(I), at 2-3.

The offense applies only to camcording in a "motion picture exhibition facility," which is defined by reference to that same term in 17 U.S.C. § 101: "a movie theater, screening room, or other venue that is being used primarily for the exhibition of a copyrighted motion picture, if such exhibition is open to the public or is made to an assembled group of viewers outside of a normal circle of a family and its social acquaintances." The term includes commercial movie theaters and may also apply to generally non-public or quasi-public spaces such as a university auditorium, but only when such a venue is being used as a "public" exhibition facility at the time of the offense. *See* H.R. Rep. No. 109-33(I), at 3, *reprinted in* 2005 U.S.C.C.A.N. 222 (stating that "open to the public" is intended to refer to the particular exhibition rather than the venue generally).

- **Trafficking in counterfeit and illicit labels, and counterfeit documentation and packaging, 18 U.S.C. § 2318**

This is covered in Chapter VI of this Manual.

- **Trafficking in goods and services with counterfeit trademarks, service marks, and certification marks, 18 U.S.C. § 2320**

See Chapter III of this Manual.

- **Digital Millennium Copyright Act (DMCA), 17 U.S.C. §§ 1201-1204**

The DMCA provides criminal penalties for dismantling the electronic locks that are intended to prevent people from accessing or copying copyrighted works without permission, for trafficking in "electronic lockpicks," and for falsifying or removing copyright management information. See Chapter V of this Manual.

- **Unauthorized reception of cable and satellite service, 47 U.S.C. §§ 553, 605 and 18 U.S.C. § 2511**
- **Economic Espionage Act, 18 U.S.C. §§ 1831-1839**

For stealing trade secrets, whether copyrighted or not, see Chapter IV of this Manual.

- **Mail and wire fraud, 18 U.S.C. §§ 1341, 1343, 1346**

Although fraud schemes can involve copyrighted works, prosecutors should be wary of charging mail or wire fraud as a substitute for a criminal copyright charge in the absence of evidence of any misrepresentation or scheme to defraud. In one copyright case, in which a wire fraud charge was brought because the facts were insufficient to support a criminal copyright charge, no misrepresentation was alleged, and the district court dismissed the charge. *See United States v. LaMacchia*, 871 F. Supp. 535 (D. Mass. 1994). The judge in *LaMacchia* reasoned that the bundle of rights conferred by copyright is unique and carefully defined, precluding prosecution under the general wire fraud statute, at least when there is no fraudulent conduct on the part of the defendant. *Id.* at 544-45. The court in *LaMacchia* relied heavily on the Supreme Court's decision in *Dowling v. United States*, 473 U.S. 207 (1985). In *Dowling*, the Court overturned the defendant's conviction for interstate transportation of stolen property under 18 U.S.C. § 2314 because it found Congress' actions to be preemptive. *See Dowling*, 473 U.S. at 207; *see also* 4 *Nimmer on Copyright* § 15.05[A] at 15-34 (1999) ("*Dowling*'s lesson is that Congress has finely calibrated the reach of criminal copyright liability, and therefore, absent clear indication of Congressional intent, the criminal laws of the United States do not reach copyright-related conduct.").

While *LaMacchia* suggests that courts are unlikely to be receptive to a wire or mail fraud charge brought as a substitute for a criminal copyright charge in a case where some element of the criminal copyright charges is missing, wire or mail fraud charges may still be viable and appropriate in infringement cases that involve actual misrepresentations or schemes to defraud. *Cf. United States v. Manzer*, 69 F.3d 222, 226 (8th Cir. 1995) (holding that sale to a third party of illegal cable television descrambling devices violated federal fraud statutes); *United States v. Coyle*, 943 F.2d 424, 427 (4th Cir. 1991) (holding sale of cable television descramblers to be a scheme to defraud "because it wronged the cable companies in their 'property rights by dishonest methods or schemes'") (quoting *United States v. McNally*, 483 U.S. 350, 358 (1987)). Nevertheless, in the absence of strong evidence of misrepresentation, prosecutors should avoid a wire or mail fraud charge if an infringement crime can be proved.

For a more detailed discussion of 18 U.S.C. §§ 1341 and 1343, refer to USAM Chapter 9-43.000. The Criminal Division's Fraud Section at (202) 514-7023 can provide further information and guidance.

- **Interstate transportation and receipt of stolen property or goods, 18 U.S.C. §§ 2314-2315**

The Interstate Transportation of Stolen Property Act ("ITSP") punishes "[w]hoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud," 18 U.S.C. § 2314, and "[w]hoever receives, possesses, conceals, stores, barters, sells, or disposes" stolen property that has crossed a state or federal boundary, 18 U.S.C. § 2315.

Although ITSP can be used under certain circumstances to prosecute theft of proprietary information or other types of intellectual property, the Supreme Court has rejected the use of the ITSP statute to prosecute copyright infringement cases, at least when the infringement does not involve the actual theft of a tangible good. *Dowling v. United States*, 473 U.S. 207 (1985). In *Dowling*, the Court reversed a conviction for the interstate transportation of infringing copies of Elvis Presley records, holding that Congress did not intend § 2314 to criminalize copyright infringement. The Court reasoned that a copyright infringer neither assumed physical control over the copyright nor wholly deprived the owner of its use. The statute "seems clearly to contemplate a physical identity between the items unlawfully obtained and those eventually

transported, and hence [requires] some prior physical taking of the subject goods." *Id.* at 216.

Despite *Dowling*, an ITSP charge may be appropriate for acts of infringement that involve the actual transportation of tangible objects across state lines. For more on these issues, see Section F. of Chapter IV of this Manual.

- **Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. §§ 1961-1968**

The criminal copyright and bootleg recordings of live music performances offenses are RICO predicates. *See* 18 U.S.C. § 1961(1)(B). RICO charges must be approved by the Department's Organized Crime and Gang Section, which can be reached at (202) 514-3594.

- **Money laundering, 18 U.S.C. § 1956**

Criminal copyright infringement is a specified unlawful activity for purposes of the money laundering statute. *See* 18 U.S.C. § 1956(c)(7)(D).

III. Trafficking In Counterfeit Trademarks, Service Marks, and Certification Marks—18 U.S.C. § 2320

A. Introduction

1. Overview

Trademarks and service marks are part of the fabric of American society. They are on our clothes, our cars, and nearly everything else we buy; they are advertised on the street, in magazines, on television and websites, and especially in stores. They are protected not only by civil law, but also by the criminal counterfeit marks statute first enacted in 1984, 18 U.S.C. § 2320.

A trademark is "any word, name, symbol, or device, or any combination thereof ... used by a person ... to identify and distinguish his or her goods ... from those manufactured or sold by others and to indicate the source of the goods." 15 U.S.C. § 1127. A service mark, by contrast, identifies the source of services rendered or offered, such as athletic events, television shows, restaurant services, telecommunications services, or retail business services, rather than goods. *Id*. Examples of well-known trademarks include Kodak®, Apple®, Microsoft®, Coca-Cola®, GE®, Life-Savers®, USA Today®, KLEENEX®, the color pink for Owens Corning fiberglass, and the NBC chime. Well-known service marks include Merry Maids®, Greyhound®, Wal-Mart®, Taco Bell®, Burger King®, and McDonald's®.

Two other types of marks are protected by 18 U.S.C. § 2320: certification and collective marks. A certification mark is used to certify characteristics of goods or services, including regional or other origin, material, mode of manufacture, quality, and accuracy. Certification marks are also used to certify that the work or labor on the goods or services was performed by members of

a union or other organization. 15 U.S.C. § 1127. Examples of certification marks include Underwriters Laboratories' UL® mark, which certifies the safety standards of electrical cable equipment, and the Woolmark® symbol, which certifies that certain laundry products can wash and dry wool and wool-blend products without damage. These marks indicate that authorized persons will manufacture the products in accordance with the mark-holder's processes. A collective mark is a trademark or service mark used by an association, union, or other group either to identify the group's products or services, or to signify membership in the group. *Id.* PGA®, Realtor®, and AFL-CIO® are examples of collective marks.

As is discussed in more detail below, the law protects marks from infringement because they are important to businesses and for consumer protection. Americans rely on the brands these marks represent when deciding which goods and services to purchase and use. This gives companies a strong incentive to control the quality of their goods and services and to invest heavily in their brands. One who infringes a mark often misleads consumers, diverts sales from the mark's owner, and misrepresents to the public the quality of the marked products and services. Criminal prosecution is appropriate for the most egregious infringers.

This Chapter first discusses the functions protected by trademarks, service marks, and certification marks. It then discusses the criminal counterfeiting statute and the elements of the crime, as well as common defenses, issues unique to this crime, and related statutory penalties. Sample indictments and jury instructions are provided in Appendix C.

The criminal counterfeit marks statute, 18 U.S.C. § 2320, and its associated statutes, have undergone several significant amendments since 2005. The Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1, 120 Stat. 285, 285-88 (2006) and the Protecting American Goods and Services Act of 2005, Pub. L. No. 109-181, § 2, 120 Stat. 285, 288 (2006) (the "2006 amendments"), effective March 16, 2006, expanded and clarified the definition of "trafficking," and added language criminalizing trafficking in labels and packaging bearing counterfeit marks, even where those labels are unattached to actual goods.

The Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act, Pub. L. No. 110-403, 122 Stat. 4256, 4261-63 (2008), effective October 13, 2008, further amended § 2320 and associated statutes addressing

counterfeiting, by (i) enhancing penalties for knowingly or recklessly causing or attempting to cause serious bodily injury or death, 18 U.S.C. § 2320(a)(2)(A) and (B) [now § 2320(b)(2)(A) and (B)]; (ii) prohibiting transshipment or exportation of goods or services, the trafficking of which was already prohibited by 18 U.S.C. § 2320(h) [now § 2320(i)]; and (iii) harmonizing forfeiture and restitution provisions under 18 U.S.C. §§ 2323 and 2320(b) [now § 2320(c)].

Most recently, the National Defense Authorization Act (NDAA) for Fiscal Year 2012, Pub. L. No. 112-81, 125 Stat. 1298 (2011), H.R. 1540, S. 1867, enacted December 31, 2011, and the Food and Drug Administration Safety and Innovation Act (FDASIA), Pub. L. No. 112-144, 126 Stat. 993, S. 3197, enacted July 9, 2012, included a number of substantial amendments to § 2320. For example, the NDAA, in § 818, amended § 2320 to include new, enhanced penalties for certain offenses involving "counterfeit military goods," a new category also defined in the NDAA. Section 2320 also now provides an express conspiracy provision, so that conspiracies to traffic in counterfeit goods may be prosecuted under § 2320 alone, rather than in conjunction with 18 U.S.C. § 371. In addition to these substantive changes to § 2320, the NDAA also restructured the offense language in § 2320(a). The FDASIA amended § 2320 to create a new offense for "trafficking in counterfeit drugs," and included new, enhanced penalties for this offense. *See* FDASIA § 717. Prosecutors should consult the text of § 2320 carefully to ensure that they are applying the law in effect at the time of the offense. Particularly in light of the recent restructuring of § 2320(a), prosecutors should be mindful that previously-used charging instruments, jury instructions, and other documents drafted prior to 2012 may use slightly different statutory language or numbering than is currently applicable. For example, the definition of "counterfeit mark" previously found in § 2320(e)(1) is now found in § 2320(f)(1).

In addition to this Chapter, prosecutors may refer to the leading treatise on trademark law, J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* (4th ed. 2012), as well as other helpful law review articles and treatises such as Ronald D. Coenen Jr. et. al., *Intellectual Property Crimes,* 48 Am. Crim. L. Rev. 849 (2011); Louis Altman & Malla Pollack, *Callmann on Unfair Competition, Trademarks and Monopolies*, 4 Callmann on Unfair Comp., T. & Mono. § 22:33 (4th ed. 2012); and David J. Goldstone & Peter J. Toren, *The Criminalization of Trademark Counterfeiting*, 31 Conn. L. Rev. 1 (1998).

Although § 2320 criminalizes the infringement of trademarks, service marks, and certification marks, for ease of discussion this Manual often refers

primarily to trademarks and sales of goods. The legal analysis should, however, apply equally to service and certification marks as well.

2. Why Criminal Law Protects Trademarks, Service Marks, and Certification Marks

Trademarks and service marks serve at least four functions:

1. They identify a particular seller's goods or services and distinguish them from those sold by others.
2. They signify that all goods or services bearing the mark come from or are controlled by a single source.
3. They signify that all goods or services bearing the same mark are of an equal level of quality.
4. They serve as a primary method to advertise and sell goods and services.

See 1 J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* § 3:2 (4th ed. 2012). A trademark or service mark also serves as an important "objective symbol of the good will that a business has built up. Without the identification function performed by trademarks, buyers would have no way of returning to buy products that they have used and liked." *Id.* Certification marks are intended to "certify regional or other origin, material, mode of manufacture, quality, accuracy or other characteristics of such person's goods or services." 15 U.S.C. § 1127.

Because "penalties under [the civil Lanham] Act have been too small, and too infrequently imposed, to deter counterfeiting significantly," much of the conduct that formerly had been subject only to civil penalties was criminalized through the enactment of the Trademark Counterfeiting Act of 1984, Pub. L. No. 98-473, 98 Stat. 2178 (1984), (codified at 18 U.S.C. § 2320). *See* S. Rep. No. 98-526, at 5 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3627, 3631.

The criminalization of trademark counterfeiting serves at least four important purposes:

a. Protecting a mark-holder's intellectual property from theft or dilution

Stealing a company's name or brand name is a type of corporate identity theft. *See* H.R. Rep. No. 109-68, at 8 n.2 (2005) ("Congress was concerned ... that counterfeiters can earn enormous profits by capitalizing on the reputations, development costs, and advertising efforts of honest manufacturers at little expense to themselves.") (alterations in original and internal quotation marks omitted) (legislative history to Stop Counterfeiting in Manufactured Goods

Act, Pub. L. No. 109-181, § 1, 120 Stat. 285 (2006)) (citing *United States v. Hon*, 904 F.2d 803, 806 (2d Cir. 1990) and S. Rep. No. 98-526, at 4-5 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3627, 3630-31). A counterfeiter should no more be able to steal a company's good name (and the profits associated with its name) than the company's money or other assets. Diane Kiesel, *Battling the Boom in Bogus Goods,* 71-MAR A.B.A.J. 60 (1985). Also, by selling inferior products, the counterfeiter may devalue a mark-holder's good name even while profiting from it. *Id*. at 61.

b. Protecting consumers from fraud

When consumers decide what goods to buy, they should be able to rely on individual goods' trademarks and the quality those marks purport to represent. *See* H.R. Rep. No. 109-68, at 8 n.2 ("Congress was concerned not only that trademark counterfeiting defrauds purchasers, who pay for brand-name quality and take home only a fake...") (alterations in original and internal quotation marks omitted) (citing *Hon*, 904 F.2d at 806 and S. Rep. No. 98-526, at 4-5); Note, *Badwill,* 116 Harv. L. Rev. 1845 (2003). Counterfeit marks can mislead consumers. They give the ring of authenticity to goods of lower quality. They can even mask serious health or safety risks to consumers, as in the cases of counterfeit food products, batteries, prescription drugs, or automotive parts. S. Rep. No. 98-526, at 4-5. Trademark counterfeiting can also be difficult to regulate civilly. With a large number of victims across a potentially large geographic region—especially in the case of goods offered online—and small losses per victim, a large-scale counterfeiter can often evade civil sanctions.

c. Protecting the safety of non-purchasing users

Sales of counterfeit products can hurt not only the trademark holder and the initial purchaser, but also third parties who use the goods or services after the initial purchase. For example, airline passengers are victims of counterfeit airplane parts, coronary patients are victims of counterfeit heart pumps, and children are victims of counterfeit infant formula, even though in each case the counterfeit goods were purchased for those consumers' benefit by another person. These are some of the types of situations that Congress sought to eradicate by criminalizing trademark infringement. *See* H.R. Rep. No. 104-556, at 3 (1996), *reprinted in* 1996 U.S.C.C.A.N. 1074, 1076; S. Rep. No. 98-526, at 4-5.

d. Enforcing market rules

Just as counterfeiting money and forging financial instruments undermine fundamental rules of the marketplace, counterfeiting trademarks weakens modern commercial systems. David J. Goldstone & Peter J. Toren, *The Criminalization of Trademark Counterfeiting*, 31 Conn. L. Rev. 1, 17-19 (1998).

B. Elements

1. The Trademark Counterfeiting Crime in General

The Trademark Counterfeiting Act, 18 U.S.C. § 2320(a), states:

> (a) Offenses.— Whoever intentionally—
>
> > (1) traffics in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services,
> >
> > (2) traffics in labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature, knowing that a counterfeit mark has been applied thereto, the use of which is likely to cause confusion, to cause mistake, or to deceive,
> >
> > (3) traffics in goods or services knowing that such good or service is a counterfeit military good or service the use, malfunction, or failure of which is likely to cause serious bodily injury or death, the disclosure of classified information, impairment of combat operations, or other significant harm to a combat operation, a member of the Armed Forces, or to national security, or
> >
> > (4) traffics in a counterfeit drug,
>
> or attempts or conspires to violate any of paragraphs (1) through (4) shall be punished as provided in subsection (b).

In contrast to criminal copyright thresholds, selling just one counterfeit item can be a felony. *United States v. Foote*, 413 F.3d 1240, 1246 (10th Cir. 2005). There is no misdemeanor provision.

Thus, to establish a criminal offense under 18 U.S.C. § 2320(a)(1)-(3), the government must prove the following elements:

1. The defendant *intentionally trafficked or attempted or conspired to traffic* in goods or services (or labels, documentation or packaging for goods or services); and
2. The defendant *knowingly used a counterfeit mark* on or in connection with those goods or services, or a counterfeit mark was applied to labels, documentation, or packaging for those goods or services.

The elements above apply to all offenses under § 2320, whether under subsection (1), (2), or (3). To prove an offense under the military counterfeits provision, § 2320(a)(3), the government must also prove the following two elements:

3. The good or service bearing a counterfeit mark is a "counterfeit military good or service," meaning that the good or service is:
   a. falsely identified or labeled as meeting military specifications, *or*
   b. intended for use in a military or national security application; *and*
4. The use, malfunction, or failure of the good or service is likely to cause one or more of the following:
   a. serious bodily injury or death,
   b. the disclosure of classified information,
   c. impairment of combat operations, or
   d. other significant harm to a combat operation, a member of the Armed Forces, or to national security.

With respect to the counterfeit drug provision, § 2320(a)(4), this provision makes it an offense to *intentionally traffic or attempt or conspire to traffic* in a "counterfeit drug"; "counterfeit drug" is defined in § 2320(f)(6) as a drug "that uses a counterfeit mark on or in connection with the drug." Congress, however, inadvertently did not include the requirement that the government must prove that the defendant *knowingly* used a counterfeit mark on or in connection with the drug. As of this writing, Congress has not amended this provision to correct the omission of this requirement. If prosecutors seek to bring a case under § 2320(a)(4), it would be prudent for prosecutors to prove that the defendant *knowingly* used a counterfeit mark on or in connection with the drug, just as they would prove the *mens rea* for § 2320(a)(1)–(3). This approach is consistent with the legislative intent. Alternatively, prosecutors can continue to use § 2320(a)(1) to charge cases involving the knowing use of a counterfeit mark on drugs as such drugs still constitute "goods." Prosecutors can contact

CCIPS at (202) 514-1026 to obtain the latest guidance with respect to the counterfeit drug provision.

In addition to the elements of the offense, the government must also show in all cases that the counterfeit mark meets the definition of a counterfeit mark as set forth in § 2320(f). To meet the definition of a counterfeit mark, the government must show that:

1. The counterfeit mark was not genuine or authentic;
2. The counterfeit mark was *identical to or substantially indistinguishable* from a genuine mark owned by another;
3. The genuine mark was *registered* on the principal register in the United States Patent and Trademark Office;
4. The genuine mark had been *in use* by the mark-holder or its licensee;
5. The counterfeit mark was used "*on or in connection with*" the defendant's goods or services (or in the case of labels and packaging, the counterfeit mark was "applied to or used in connection with" the goods or services or was "applied to or consist[ed] of" labels, documentation, or packaging "of any type or nature");
6. The counterfeit mark was used "in connection with" *the type of goods or services for which the protected mark was registered*, (or in the case of labels and packaging, the counterfeit labels, documentation, or packaging were "designed, marketed, or otherwise intended to be used on or in connection with the goods or services for which the mark [was] registered"); and
7. The counterfeit mark was used in a manner *"likely to cause confusion, to cause mistake, or to deceive."*

These elements and definition are discussed in detail below.

2. Relevance of Civil Trademark Law in Criminal Counterfeiting Cases

When Congress drafted § 2320, it relied on the "concepts and definitions of the Lanham Act," the civil trademark statute codified at 15 U.S.C. §§ 1051-1127. *See* H.R. Rep. No. 98-997, at 4-5 (1984). The Lanham Act's defenses and limitations on remedies are specifically incorporated into § 2320, *see* 18 U.S.C. § 2320(d), (f)(3), and are discussed in Section C.4. of this Chapter. Moreover, Congress repeatedly indicated that the Lanham Act was the background against which § 2320 should be interpreted. *See, e.g.*, *Joint Statement on Trademark Counterfeiting Legislation*, 130 Cong. Rec. 31,675 (1984) (hereinafter "*Joint*

Statement") ("No conduct will be criminalized by this act that does not constitute trademark infringement under the Lanham Act.").

Given this legislative history, courts deciding criminal cases under § 2320 have often turned to civil opinions decided under the Lanham Act. For example, the Ninth Circuit affirmed a defendant's § 2320 conviction by relying not only on the criminal statute's legislative history, but also on two civil Lanham Act cases. The court noted that the "definition of the term 'counterfeit mark' in the Lanham Act is nearly identical to the definition [of counterfeit mark] in Section 2320, suggesting that Congress intended to criminalize all of the conduct for which an individual may be civilly liable." *United States v. Petrosian*, 126 F.3d 1232, 1234 (9th Cir. 1997); *see also* 15 U.S.C. §§ 1116(d) (defining "counterfeit mark" in civil actions), 1127 (defining "counterfeit"). Similarly, the Eleventh Circuit held that the "likely to cause confusion, mistake or deceive" test within the definition of counterfeit mark at 18 U.S.C. § 2320(f)(1)(A)(iii) extends beyond direct purchasers to encompass the purchasing public and potential purchasers based on the "identical language" in the Lanham Act and the legislative history. *United States v. Torkington*, 812 F.2d 1347, 1352 (11th Cir. 1987) ("Congress ... manifested its intent that [§ 2320] be given the same interpretation as is given the identical language in [§] 1114(1) of the Lanham Act").

Despite the civil and criminal laws' many similarities, some courts have held that their differences sometimes merit distinction. *See United States v. Hanafy*, 302 F.3d 485, 488 (5th Cir. 2002) (holding that Lanham Act cases "should not be used as authoritative in interpreting a criminal statute"); *United States v. Giles*, 213 F.3d 1247, 1249-50 (10th Cir. 2000) (declining to follow a civil case in part because § 2320, as a criminal statute, must be construed more narrowly); *Torkington*, 812 F.2d at 1350 (noting that § 2320 is "narrower in scope" than the Lanham Act).

3. Intentionally Trafficked in Goods or Services (or Labels, Documentation, or Packaging for Goods or Services)

Section 2320(a) requires the government to prove that the defendant "intentionally" trafficked in goods or services or in "labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature," or attempted or conspired to do so. 18 U.S.C. § 2320(a)(1), (2).

a. Intentionally

The term "intentionally" modifies "traffics." *See* Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1, 120 Stat. 285, 285-87 (2006); *United States v. Baker*, 807 F.2d 427, 429 (5th Cir. 1986) (quoting legislative history's breakdown of § 2320's two mens rea elements). It means "that the defendant trafficked in the goods or services in question deliberately, or 'on purpose.'" *See Joint Statement,* 130 Cong. Rec. 31,674 (1984).

As a general intent crime, the government need not prove that the defendant specifically intended to violate 18 U.S.C. § 2320 or even that he knew his conduct was illegal. *Baker*, 807 F.2d at 427-30; *United States v. Gantos*, 817 F.2d 41, 42-43 (8th Cir. 1987) (affirming district court's refusal to instruct jury that § 2320 required proof that defendant knew that his act violated the law).

b. Trafficked

i. General Definition

"Traffic" is broadly defined in § 2320(f)(5) to mean "to transport, transfer, or otherwise dispose of, to another, for purposes of commercial advantage or private financial gain, or to make, import, export, obtain control of, or possess, with intent to so transport, transfer, or otherwise dispose of." The current definition resolves some difficulties that arose from earlier definitions used in the statute, which turned on the meaning of "consideration."

Prior to March 16, 2006, "traffic" was defined somewhat more narrowly, in what was then subsection (e)(2) of 18 U.S.C. § 2320 to mean "transport, transfer, or otherwise dispose of, to another, as consideration for anything of value, or make or obtain control of with intent so to transport, transfer, or dispose of." That definition was intended to be broad, covering all aspects of commercial activity from initial manufacture to distribution and sale, but it was not intended to cover purchases for personal use. *See Joint Statement*, 130 Cong. Rec. 31,675 (1984); S. Rep. No. 98-526 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3627; David J. Goldstone & Peter J. Toren, *The Criminalization of Trademark Counterfeiting*, 31 Conn. L. Rev. 1 (1998). A defendant who did not personally "transport[], transfer[], or otherwise dispose[]" of the goods but who aided and abetted a co-conspirator who did traffic could be convicted as an aider-and-abettor. *See United States v. Guerra*, 293 F.3d 1279, 1287 (11th Cir. 2002) (affirming § 2320 conspiracy and aiding-and-abetting convictions

for defendants who made labels that a co-conspirator attached to fake Cuban cigars he sold).

Yet the pre-2006 definition arguably covered too narrow a swath of commercially-motivated conduct, and it generally did not explain how to deal with cases in which the defendant was caught possessing counterfeits with the intent to traffic in them. See Sections B.3.b.ii.-iii. of this Chapter.

These problems were fixed by the Protecting American Goods and Services Act of 2005, enacted March 16, 2006. The statute modified the definition of the term "traffic" to (1) clarify that it includes trafficking committed for commercial purpose or financial gain (which includes the receipt or expected receipt of anything of value); (2) applies to importing or exporting counterfeit goods; and (3) includes possession with intent to transport, transfer or otherwise dispose of. *See* Pub. L. No. 109-181, § 2, 120 Stat. 285, 288 (2006) (amending the former 18 U.S.C. § 2320(e)(2), (3) (now numbered 2320(f)(5), (f)(2), respectively). These issues are discussed below.

ii. Consideration vs. Commercial Advantage and Private Financial Gain

Under the pre-2006 definition of "traffic," the thing "of value" that a defendant had to receive as consideration for the counterfeit goods did not need to be a financial payment, but rather could be anything that had value. *See United States v. Koehler*, 24 F.3d 867, 870-71 (6th Cir. 1994) (affirming § 2320 conviction based on acceptance of air conditioner compressors in lieu of financial payment). That rule survived the 2006 amendments, in which "consideration" was replaced with "for purposes of commercial advantage or private financial gain," § 2320(e)(2) (as amended), and "financial gain" was defined as including "the receipt, or expected receipt, *of anything of value*," § 2320(e)(3) (as amended) (emphasis added) (now numbered 2320(f)(5), (f)(2), respectively).

The "consideration" requirement may have been too narrow to capture some types of commercially-motivated counterfeiting conduct. For example, at least one court held that the term "consideration" must be interpreted in the contractual sense as the product of a bargained-for exchange between parties. *See United States v. Habegger*, 370 F.3d 441, 444-45 (4th Cir. 2004). In *Habegger*, the Fourth Circuit held that a free sample of counterfeit goods sent to a potential customer did not constitute "trafficking" under what was then § 2320(e)(2) (now § 2320(f)(2)), even if the samples had been sent to

maintain the customer's good will, because there had been no agreement to purchase goods. *Id.* at 445. The court might have decided differently, however, had there been "more than a mere hope on the part of the sender that the recipient [would] purchase goods in the future," such as if the recipient had "promised to pay for the socks, to buy additional socks if he found the samples acceptable, or even to examine the socks and consider purchasing more." *Id.*

To avoid problems like this, Congress replaced "consideration" with "for purposes of commercial advantage or financial gain," a phrase which has a long-standing meaning within the copyright and criminal codes. It covers a wider variety of profit-related infringement, regardless of whether the defendant infringed for a direct *quid pro quo* or actually made a profit. For a detailed discussion of how to apply the commercial advantage or financial gain element, see Section B.4. of Chapter II of this Manual.

The post-2006 definition of "traffic" in § 2320 is sufficiently broad to cover virtually all types of commercial transactions, but does not extend to a consumer's acquisition of a counterfeit item solely for personal use. This was also true under the prior version of "traffic." *See Joint Statement*, 130 Cong. Rec. 31,675 (1984).

iii. Making and Obtaining Counterfeits vs. Possession with Intent to Traffic

At first glance, possession of contraband with intent to traffic—which the old definition did not explicitly cover—appears coextensive with making or obtaining control of contraband with intent to traffic—both of which the old and new definitions explicitly included. *See* 18 U.S.C. § 2320(f)(5); *United States v. DeFreitas*, 92 F. Supp. 2d 272, 277 (S.D.N.Y. 2000) (holding that purchasing counterfeit items in China for transportation to and sale in the United States constituted an illegal act of "obtaining control" for purposes of § 2320).

Yet there is a subtle—but important—distinction between "obtaining control" with intent to traffic and "possession" with intent to traffic. Consider a warehouse full of counterfeits, with no records indicating when the counterfeits were made, obtained, or transported. Under the old definition of trafficking, the defendant might argue that although the government could show that he *possessed* counterfeits in commercial quantities, it could not prove when he *made* or *obtained control* of them—the old definition's operative verbs. In the same vein, the defendant might argue that without records to prove

when the defendant made or obtained control of the counterfeits, *a fortiori* the government could not prove that these events occurred within the statute of limitations. If, however, the government need only prove that the defendant *possessed* the contraband with the intent to traffic in it, then the government can establish that that action occurred on the date it found the warehouse full of counterfeits; it need not prove when the defendant acquired or produced the contraband. Thus, Congress amended the definition of trafficking explicitly to include possession with intent to traffic.

iv. Importing and Exporting Related to Transporting

Congress added importing and exporting to the new definition of trafficking in 2006 to make clear that both acts violate § 2320. The pre-2006 definition of "traffic" covered both importing and exporting counterfeits: importing and exporting are forms of transporting goods, and the old definition explicitly covered transportation. *See* 18 U.S.C. § 2320(e)(2) (2000) ("[T]he term 'traffic' means to *transport*, transfer, or otherwise dispose of, to another ...") (emphasis added) (pre-2006 amendments); *DeFreitas*, 92 F. Supp. 2d at 276-77 (holding that importing counterfeit items from China into the United States for sale constituted trafficking under § 2320). The 2006 amendments make it even clearer that the acts of importing and exporting counterfeits violate § 2320.

c. Goods and Services (and Labels, Patches, Stickers, Wrappers, Badges, Emblems, Medallions, Charms, Boxes, Containers, Cans, Cases, Hangtags, Documentation, or Packaging of Any Type or Nature)

Before the 2006 amendments, § 2320 only criminalized trafficking in counterfeit "goods" or "services" (which continue to be criminalized under § 2320(a)(1) and (a)(3)). In the 2006 amendments, Congress expanded § 2320 to criminalize trafficking in labeling and packaging components designed to be applied to accompany goods or services.

Neither § 2320 nor the Lanham Act define the terms "goods or services." Section 2320's legislative history, however, provides some guidance regarding the meaning of "goods." In the legislative history, Congress's focus was on the damage caused by various types of counterfeit goods such as drugs, automobile parts, cosmetics, fertilizers, computer parts, and medical devices. H.R. Rep. No. 98-997, at 5 (1984). With regard to "services," however, the legislative histories for § 2320 and the Lanham Act are silent. *See In re Advertising & Marketing Dev., Inc.*, 821 F.2d 614, 618 (Fed. Cir. 1987) (discussing Lanham Act's legislative history). Although courts have not defined "services" under

§ 2320, in Lanham Act cases, courts have defined the term broadly to include "the performance of labor for the benefit of another." *In re Canadian Pac. Ltd.*, 754 F.2d 992, 994 (Fed. Cir. 1985) (emphasis omitted); *Morningside Group Ltd. v. Morningside Capital Group, L.L.C.*, 182 F.3d 133, 137-38 (2d Cir. 1999).

The difficulty with punishing defendants for using counterfeit marks only in connection with goods and services for which the genuine mark was registered was that it created a potential loophole for trafficking in labels, documentation, and packaging with counterfeit marks. Labels, documentation, and packaging that bore counterfeit trademarks but which were unattached to other goods or services ran the possibility of not being considered "goods" under § 2320 if the mark-holder had not registered the marks for use on labels, documentation, and packaging.

This was the holding of the Tenth Circuit in *United States v. Giles*, 213 F.3d 1247, 1253 (10th Cir. 2000) ("Section 2320 does not clearly penalize trafficking in counterfeit labels which are unattached to any goods."). In *Giles*, the defendant sold patches bearing counterfeit Dooney & Burke trademarks. The patches could be attached to generic handbags and luggage to make them counterfeit, but Dooney & Burke had registered the marks for use on handbags and luggage, not on patches, and the defendant did not sell the fake handbags and luggage to which the patches were to be attached. The Tenth Circuit concluded that the patches were labels, not goods, and that the defendant could not be convicted under § 2320 for trafficking in unattached labels. The court indicated, however, that the case might have been decided differently had the marks been registered for use on patches or if the defendant had been charged with aiding-and-abetting trafficking in counterfeit goods. *Id.* at 1251 n.6, 1252 & n.7. Thus, a defendant who used a counterfeit mark but did not provide the good or service himself generally had to be charged under § 2320 in conjunction with conspiracy or aiding-and-abetting. *Id.* at 1251 n.6; *United States v. Guerra*, 293 F.3d 1279, 1286-87 & n.4 (11th Cir. 2002) (affirming conviction on these grounds).

Congress directly addressed the *Giles* decision by amending § 2320 to expressly criminalize trafficking in counterfeit labels, documentation, and packaging directly:

> Whoever intentionally traffics or attempts to traffic in goods or services and knowingly uses a counterfeit mark on or in

> connection with such goods or services[, or intentionally traffics or attempts to traffic in labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature, knowing that a counterfeit mark has been applied thereto, the use of which is likely to cause confusion, to cause mistake, or to deceive,] shall, if an individual, be fined not more than $2,000,000 or imprisoned not more than 10 years, or both, and, if a person other than an individual, be fined not more than $5,000,000.

18 U.S.C. § 2320(a) (2006) (bracketed language inserted by the Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1(b)(1), 120 Stat. 285, 285 (2006)); *see* H.R. Rep. No. 109-68, at 7 ("This modification is intended to overrule the holding in the case *United States v. Giles* ...."). Thus, beginning in 2006, defendants could be charged with trafficking in labels, documentation, and packaging with counterfeit marks under § 2320 without resort to aiding-and-abetting or conspiracy charges.

Despite the focus on labels, documentation, or packaging that bear inauthentic marks, repackaging authentic goods with inauthentic labels is criminal only in a limited set of circumstances. See Sections C.3. and D.4. of this Chapter.

A defendant can be convicted for trafficking in a single good, service, label, piece of documentation or packaging. *See United States v. Foote*, 413 F.3d 1240, 1246-47 (10th Cir. 2005) (holding that § 2320's use of "goods" in the plural does not preclude prosecution of a person who traffics in a single counterfeit good).

Whether the things that the defendant trafficked in consist of "goods" or "services"—or as labels, documentation, or packaging intended to be used with goods or services—is governed by the victim's certificate of registration with the United States Patent and Trademark Office. The certificate of registration will indicate whether the mark in question had been registered for goods or for services and, if so, for what class of good or service. See Section B.4.c. of this Chapter.

4. The Defendant Used a "Counterfeit Mark": Definition of a Counterfeit Mark

The government must prove that the defendant knowingly used a "counterfeit mark" on or in connection with goods or services, or that a counterfeit mark was applied to the labels, documentation, or packaging. 18 U.S.C. § 2320(a). To prove this element, the government must also demonstrate that the counterfeit mark in question meets the statutory definition of a counterfeit mark in 2320(f)(1)(A).

a. Not Genuine or Authentic

"Counterfeit mark" is a term of art that is defined as follows:

> (A) a spurious mark—
>
> > (i) that is used in connection with trafficking in any goods, services, labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature;
> >
> > (ii) that is identical with, or substantially indistinguishable from, a mark registered on the principal register in the United States Patent and Trademark Office and in use, whether or not the defendant knew such mark was so registered;
> >
> > (iii) that is applied to or used in connection with the goods or services for which the mark is registered with the United States Patent and Trademark Office, or is applied to or consists of a label, patch, sticker, wrapper, badge, emblem, medallion, charm, box, container, can, case, hangtag, documentation, or packaging of any type or nature that is designed, marketed, or otherwise intended to be used on or in connection with the goods or services for which the mark is registered in the United States Patent and Trademark office; and
> >
> > (iv) the use of which is likely to cause confusion, to cause mistake, or to deceive.

18 U.S.C. § 2320(f)(1)(A).

A "spurious" mark is one that is "not genuine or authentic." *Joint Statement*, 130 Cong. Rec. 31,675 (1984).

Although this definition appears to indicate that the mark itself must be counterfeit, rather than the goods or services (or, in a labels case, the labels, documentation, or packaging), it is well-settled that a genuine or authentic mark becomes counterfeit when it is used in connection with something else that is counterfeit. *See* 4 J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* § 25:15 (4th ed. 2012); *United States v. Petrosian*, 126 F.3d 1232 (9th Cir. 1997). In *Petrosian*, the defendant, who filled genuine Coca-Cola bottles with a substitute carbonated beverage and sold it as Coca-Cola, contended that his Coca-Cola marks were not counterfeit because his genuine bottles bore genuine marks. 126 F.3d at 1233. The Ninth Circuit disagreed, holding that "[w]hen a genuine trademark is affixed to a counterfeit product, it becomes a spurious mark.... The Coca-Cola mark became spurious when [defendant] affixed it to the counterfeit cola because the mark falsely indicated that Coca-Cola was the source of the beverage in the bottles and falsely identified the beverage in the bottles as Coca-Cola." *Id.* at 1234. See also Section C.3. of this Chapter concerning the repackaging of authentic goods. This rule should apply equally to services, labels, documentation, and packaging.

The definition of "counterfeit mark" in § 2320(f)(1)(B) also includes designations protected by the Olympic Charter Act. See Section D.8. of this Chapter.

Separate laws punish the counterfeit use of emblems, insignias, and names of:

- military medals and designations;
- veterans' organizations;
- cremation urns for military use;
- the seals of the United States President, Vice President, Senate, House of Representatives, and Congress;
- federal agencies;
- the Department of Interior's golden eagle insignia;
- police badges;
- the Red Cross;
- the 4-H club;
- the Swiss Confederation;
- Smokey the Bear; and

- Woodsy the Owl.

See 18 U.S.C. §§ 700-716.

b. The Counterfeit Mark Must Be Identical to or Indistinguishable from a Genuine Mark Owned by Another

Under 18 U.S.C. § 2320(f)(1)(A), a counterfeit mark is a spurious mark that is "identical with, or substantially indistinguishable from," a federally registered mark. This standard is based on the same standard set forth in the Lanham Act, 15 U.S.C. § 1127. The legislative history suggests that the civil and criminal standards should be interpreted the same. *See Joint Statement*, 130 Cong. Rec. 31,675-76 (1984) (noting that the civil and criminal standards "differ slightly in their terms, but [] are identical in substance," and citing civil cases to explain both standards). To the extent the criminal and civil standards diverge at all, the criminal standard should be interpreted more narrowly only in cases at the outer margins. *United States v. Guerra*, 293 F.3d 1279, 1288 (11th Cir. 2002) (citing *Joint Statement*, 130 Cong. Rec. 31,675 (stating that § 2320 is not intended to criminalize what would have been "arguable" cases of civil trademark infringement before the criminal act's passage)). Note, however, that although the criminal and civil standards are virtually identical with respect to what constitutes a "counterfeit," civil law also prohibits the unauthorized use of a "colorable imitation of a registered mark," *see* 15 U.S.C. § 1114(1)(a), which by its terms falls short of being a counterfeit mark that is "identical with, or substantially indistinguishable from" a genuine mark. Nevertheless, "[b]ecause of the similarity between this definition and the § 2320 definition of 'counterfeit mark,' we find Lanham Act civil counterfeiting cases helpful to our analysis of criminal counterfeiting cases brought under § 2320(a)." *United States v. Lam*, 677 F.3d 190, 199 n.8 (4th Cir. 2012)

Whether a defendant has used a mark that is "substantially indistinguishable" from a federally registered mark is a fact question that must be determined on a case-by-case basis. *See Joint Statement*, 130 Cong. Rec. 31,675 ("the definition of 'substantially indistinguishable' will need to be elaborated on a case-by-case basis"); *cf. Colgate-Palmolive v. J.M.D. All-Star Import and Export Inc.*, 486 F. Supp. 2d 286, 291 (S.D.N.Y. 2007) ("Cases applying the 'substantially indistinguishable' test are inherently fact intensive."). Nevertheless, Congress did give the following guidance on the scope of the substantially indistinguishable standard:

> Obviously, a mark need not be absolutely identical to a genuine mark in order to be considered "counterfeit." Such an interpretation would allow counterfeiters to escape liability by modifying the registered trademarks of their honest competitors in trivial ways. However, the sponsors do not intend to treat as counterfeiting what would formerly have been arguable, but not clear-cut, cases of trademark infringement.

Joint Statement, 130 Cong. Rec. 31,676 (1984); *accord Lam*, 677 F.3d at 199 (quoting *United States v. Guerra*, 293 F.3d 1279, 1288 (11th Cir. 2002) (quoting *Joint Statement*, 130 Cong. Rec. 31,675)); *Pepe (U.K.) Ltd. v. Ocean View Factory Outlet*, 770 F. Supp. 754, 758 (D.P.R. 1991) (same); *Colgate-Palmolive*, 486 F. Supp. 2d at 289 (same). For example, in *Pepe*, the court held that a defendant uses a mark that is substantially indistinguishable from a registered mark when the similarities between the marks presents "more than an *arguable* case of infringement." 770 F. Supp. at 759 (emphasis in original). In *Montres Rolex, S.A. v. Snyder*, a case that pre-dates the enactment of § 2320 but was cited with approval in the statute's legislative history (130 Cong. Rec. at 31,675-76), the Second Circuit acknowledged that the difference between the "likely to cause confusion" and "substantially indistinguishable" standards "may be more theoretical than real" in some cases. 718 F.2d 524, 531 (2d Cir. 1983). More recently, in reviewing a jury's finding that two marks are substantially indistinguishable from one another, the Fourth Circuit held that "a good displaying an allegedly counterfeit trademark must possess *pronounced differences* from a legitimate trademarked good for us to declare that no rational jury could find that it was a counterfeit." *Lam*, 677 F.3d at 199 (emphasis added).

"In general, however, [word] marks that are similar to the registered mark, but differ by two or more letters, are not likely to be considered counterfeit," *Colgate-Palmolive*, 486 F. Supp. 2d at 291, suggesting that marks that differ in only one letter may be considered counterfeit. For example, use of the mark "Prastimol" for a medication that is the functional equivalent of the product sold under the trademark "Mostimol" would not be a crime. *Joint Statement*, 130 Cong. Rec. 31,676. Nor would a 'P' superimposed over a 'V' on a fleur-de-lis pattern be substantially indistinguishable from an 'L' superimposed over a 'V' over the same pattern, or using "Amazonas" rather than "Amazon," or "Bolivia" rather than "Bulova." *See Montres Rolex*, 718 F.2d at 531-32 (noting that these examples might create a likelihood of confusion without being

substantially indistinguishable, in case interpreting Customs's power to seize counterfeits).

A counterfeiter who sells a look-alike with an altered brand name can still be convicted, however, if his look-alike reproduces other registered trademarks. *See United States v. Yi*, 460 F.3d 623, 627 n.1, 629 n.4 (5th Cir. 2006) (holding that even though defendant's batteries were named "Dinacell" rather than "Duracell," the batteries were still counterfeit because they used Duracell's copper-top and black-body trademark). Likewise, a counterfeiter who sells a look-alike with an altered trademarked design can still be convicted if the look-alike reproduced another registered design mark. *Lam*, 677 F.3d at 198-99 (rejecting defendant's argument that "[n]o rational jury would conclude that a mark with a knight integrated onto it was a counterfeit of a mark without a knight" and holding that a rational jury could find that defendant's mark bearing a plaid and an equestrian knight was substantially indistinguishable from Burberry's federally registered plaid or "Check" mark without a knight, "especially in light of the evidence demonstrating that Burberry often sells goods displaying the Burberry Check mark and the Burberry Equestrian mark together") (internal quotation marks omitted).

Prosecutors should pay special attention to word marks. A trademark can consist of a symbol, a picture, or a stylized depiction of a word (such as the distinctive Coca-Cola® cursive mark). A trademark can also consist of a simple word. A word mark registered in a neutral font and all capital letters "covers *all* design features and is not limited to any special form or lettering." *Sally Beauty Co. v. Beautyco, Inc.*, 304 F.3d 964, 970 (10th Cir. 2002) (emphasis added) (citations omitted); 3 J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* § 19:58 (4th ed. 2012) ("'Registrations with typed drawings are not limited to any particular rendition of the mark and, in particular, are not limited to the mark as it is used in commerce.'") (quoting *Cunningham v. Laser Golf Corp.*, 222 F.3d 943, 950 (Fed. Cir. 2000)); *see also Cunningham*, 222 F.3d at 949-50; 37 C.F.R. § 2.52 (2012). In other words, there is a strong argument that a mark registered in this manner is counterfeited by any infringing use of the mark, whether in the font used by the mark-holder or not, because the infringing word mark is substantially indistinguishable from the word mark itself.

When trying to determine which trademarks the defendant infringed, prosecutors and agents should consult with the victim. Although the government itself can search for trademarks on the United States Patent and

Trademark Office's website, these searches can be cumbersome. Given the range of perceptible elements that can be registered as marks—witness the color pink for Owens Corning fiberglass, the NBC chime, the Burberry plaid, and the shape of the Coca-Cola bottle (respectively U.S. Trademark Reg. Nos. 1439132 and 2380742, 0916522, 2022789, and 1057884)—the victim is best suited to identify which elements were registered as marks and which may have been counterfeited.

Section 2320 does not specify the procedure for establishing at trial that the counterfeit mark is identical to or substantially indistinguishable from a genuine registered mark. *See Guerra*, 293 F.3d at 1288. In *Guerra,* the Eleventh Circuit rejected the defendant's contention at trial that the government must 1) introduce genuine trademarks affixed to genuine goods, 2) introduce the testimony of a representative from the mark-holder, and 3) rely on investigative agents who are experts in the counterfeited product or service. *Id.*; *see also United States v. Able Time, Inc.*, 545 F.3d 824, 836 (9th Cir. 2008) (rejecting the proposition that a factfinder must compare the alleged counterfeit mark with the registered mark as it appears on actual merchandise and holding that "[o]n remand, the factfinder may compare the offending mark to the mark on the registration certificate"). Instead, the Eleventh Circuit ruled that introducing registered trademark designs and labels produced by authorized licensees was sufficient. *Guerra*, 293 F.3d at 1288. Other courts have approved the government's use of expert testimony and a comparison between counterfeit and genuine goods. *See United States v. Yamin*, 868 F.2d 130, 135 (5th Cir. 1989); *United States v. McEvoy*, 820 F.2d 1170, 1172 (11th Cir. 1987) (same). Prosecutors should note that courts have declined to adopt the point of view of experts in determining whether defendants used marks that are substantially indistinguishable from federally registered marks. *Montres Rolex*, 718 F.2d at 531 (holding that the same "average purchaser test" for the "likely to cause confusion" infringement standard applies to the "substantially indistinguishable" standard); *Pepe*, 770 F. Supp. at 758 ("The court in the *Rolex* case made the determination whether a mark was a substantially indistinguishable counterfeit, as opposed to a mere infringement, from the standpoint of an average purchaser rather than from the standpoint of an expert.").

In civil cases, courts have also allowed evidence of actual confusion, such as customers who were fooled, and trademark surveys. 4 J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* §§ 23:2, 13, 17, 63 (4th ed. 2012). Market surveys are often used in civil cases, but can raise evidentiary

issues. *See, e.g.*, 6 *McCarthy on Trademarks and Unfair Competition* §§ 32:158, 170; *Citizens Fin. Group v. Citizens Nat'l Bank of Evans City*, 383 F.3d 110 (3d Cir. 2004). As of the writing of this Manual, no reported cases address the admissibility of market surveys in criminal trademark prosecutions.

The procedures and analysis for comparing counterfeit and legitimate marks are also addressed in Section B.4.g. of this Chapter, which discusses how to prove likelihood of confusion. *See Montres Rolex*, 718 F.2d at 531.

Proving that two marks are likely to be confused is not always sufficient to prove that they are identical or substantially indistinguishable. Likelihood of confusion is a lower hurdle. *See id.* at 531-32 (noting examples of marks that were likely to cause confusion, but which were not substantially indistinguishable from the real thing: a 'P' superimposed over a 'V' on a fleur-de-lis pattern vs. an 'L' superimposed over a 'V' over the same pattern; "Amazonas" vs. "Amazon"; and "Bolivia" vs. "Bulova"). For actual comparisons of marks that were alleged to be confusingly similar, see 3 *McCarthy on Trademarks and Unfair Competition* §§ 23:21-40, keeping in mind the potential differences between civil and criminal cases (see Section B.2. of this Chapter) and the difference between "likelihood of confusion" and marks being "substantially indistinguishable."

c. The Genuine Mark Must Be Federally Registered on the U.S. Patent and Trademark Office's Principal Register

The victim's mark must have been registered on the principal register in the United States Patent and Trademark Office ("USPTO"), 18 U.S.C. § 2320(f)(1)(A)(ii), unless the case involves the Olympic symbols (see Section D.8. of this Chapter).

Federal registration is a jurisdictional element. Thus, § 2320 cannot be charged if the victim's mark was only registered on the USPTO's supplemental register, recorded with Customs, registered with state agencies, or protected at common law. However, if a § 2320 charge is unavailable because the mark was not registered on USPTO's principal register, alternate charges such as mail fraud, wire fraud, or state or local trademark charges may still be available. See Section F. of this Chapter.

Proving the mark's registration is usually straightforward. Generally, the government will simply offer a certified copy of the certificate of registration. The court may take judicial notice of registration certificates. *See* Fed. R. Evid.

201(b); *Duluth News-Tribune v. Mesabi Publ'g Co.*, 84 F.3d 1093, 1096 n.2 (8th Cir. 1996); *Omega S.A. v. Omega Eng'g*, 228 F. Supp. 2d 112, 120 & n.26 (D. Conn. 2002); *cf. Island Software and Computer Serv. v. Microsoft Corp.*, 413 F.3d 257, 261 (2d Cir. 2005) (approving judicial notice of copyright registration certificates). Unofficial registration information can be searched on the USPTO's website: http://www.uspto.gov/main/trademarks.htm. Formal, certified copies of the registration certificates can be obtained directly from USPTO. The Department of Justice has no special method for expediting delivery of certificates from USPTO, beyond perhaps a grand jury or trial subpoena, which should be discouraged. The usual method is to obtain certified copies of certificates from the victims themselves.

Registration may also be proved through other means, such as testimony of the mark-holder and other circumstantial evidence. For example, in *United States v. DeFreitas,* 92 F. Supp. 2d 272, 278 (S.D.N.Y. 2000), the court allowed the jury to conclude that a mark was registered based on testimony of the mark-holder for Beanie Babies along with samples of genuine Beanie Babies with tags bearing registered tags, the mark-holder's catalogue containing a statement that the trademark was registered, and testimony of the mark-holder's CEO. In *United States v. Park*, 164 Fed. Appx. 584, 585-86 (9th Cir. 2006), the Ninth Circuit found that the government had proved registration by introducing a civil complaint against the defendant in a prior suit that she had settled, in which the complaint stated that the trademarks were registered; by introducing testimony of the defendant's civil attorney in that case, who testified that the victims were trademark owners at the time of the prior civil action; and by introducing testimony of an agent who testified that the items seized at the defendant's business were identical to items registered as trademarks in the USPTO.

Prosecutors who intend to prove registration by alternate means, however, must take care to ensure that the evidence presented is sufficiently detailed and precise. For example, in *United States v. Xu*, 599 F.3d 452, 455 (5th Cir. 2010), the Fifth Circuit vacated the defendant's conviction for trafficking in a counterfeit version of a pharmaceutical drug called Zyprexa because it concluded the government failed to prove the registration of the drug's trademark. During trial, an employee of the drug's manufacturer was shown a counterfeit container of the medication and was asked about the symbol that appeared next to the drug's name; the employee responded that it was the "registered trademark symbol." *Id.* at 454. The court concluded this

testimony was insufficient to prove registration because, as an initial matter, "the symbol being discussed was on a package of allegedly counterfeit goods, not authentic drugs, and no effort was made to demonstrate that authentic Zyprexa carried the same symbol." *Id.* Furthermore, the court explained that the mere statement that the trademark was "registered" was insufficient due to the fact that it did not specify that the registration appeared on the USPTO's principal register, as opposed to on its supplemental register, with Customs, or perhaps with a state agency. *Id.* at 455; *see also United States v. Xu*, No. H-07-362, 2008 WL 5122125, at *3-4 (S.D.Tex. Dec. 4, 2008) (explaining district court's reasoning for granting judgment of acquittal with regard to additional counts of trafficking in other counterfeit drugs due to government's failure to prove mark registration), *vacated*, 599 F.3d 452 (5th Cir. 2010).

Registration is *prima facie* evidence that the registrant owns the mark and that the registration is valid. 15 U.S.C. § 1057(b). In criminal prosecutions, the genuine mark is usually treated as "incontestable" if it has been registered on the principal register for more than five consecutive years. *See* 15 U.S.C. § 1065 (setting out conditions for "incontestability"). A federal trademark registration may, however, be canceled in whole or part in a civil judicial or administrative proceeding. *See* 15 U.S.C. § 1064.

The government need not prove that the defendant was aware that the mark was registered. 18 U.S.C. § 2320(f)(1)(A)(ii) (stating that a counterfeit mark is one that is "identical with, or substantially indistinguishable from" a registered mark "whether or not the defendant knew such mark was so registered"). *See also United States v. Guerra*, 293 F.3d 1279, 1287 (11th Cir. 2002) (holding that "it is irrelevant that [the defendant] did not know the marks were registered in the United States"); *United States v. Sung*, 51 F.3d 92, 93-94 (7th Cir. 1995) (holding that § 2320's definition of "counterfeit mark" imposes on defendants "the duty to inquire into the [registration] status of the mark") (citations omitted).

d. The Genuine Mark Must Have Been in Use by the Mark-Holder or Its Licensee

The genuine mark must also be "in use," presumably by the mark holder or his licensee, 18 U.S.C. § 2320(f)(1)(A)(ii). See Section A.1. of this Chapter, except in cases involving protected Olympic symbols, as discussed in Section D.8. of this Chapter.

The term "in use" is not defined or explained in the statute, its legislative history, or in case law. The Lanham Act, however, defines a trademark's "use in commerce" as "the bona fide use of a mark in the ordinary course of trade, and not made merely to reserve a right in a mark." 15 U.S.C. § 1127. *See also ConAgra, Inc. v. George A. Hormel, & Co.*, 990 F.2d 368, 371-72 (8th Cir. 1993) (affirming district court's finding that the trademark application was based on actual sales and not a "sham use"). Civil cases have held that "in use" means use in the United States, not in other nations. *See Marshak v. Treadwell*, 240 F.3d 184 (3d Cir. 2001); *Rivard v. Linville*, 133 F.3d 1446, 1448-49 (Fed. Cir. 1998); *see also United States v. Penton*, 303 Fed. Appx. 774, 780-81 (11th Cir. 2008) (stating that defendant was correct when he argued that because products bearing particular marks were not sold in the United States they could not be "in use" for the purposes of § 2320).

To prove that the genuine mark was in use during the offense, the government may not rely solely on a certification of registration that shows that the victim registered the trademark before the date of the offense. Registration merely requires a mark-holder to have a bona fide *intent* to use the mark, which does not translate into actual use. *United States v. Foote,* 238 F. Supp. 2d 1271, 1278 (D. Kan. 2002), *aff'd*, 413 F.3d 1240, 1248 (10th Cir. 2005); *United States v. Guerra*, 293 F.3d 1279, 1290 (11th Cir. 2002). Nor may the government establish use by relying on the jurors' probable experience with the trademark at issue, since the jurors' experience is not legal evidence. *Foote*, 238 F. Supp. 2d at 1279 n.11.

Evidence that will suffice to demonstrate a mark is "in use," however, includes proof of registration in conjunction with evidence of the first use by the mark-holder and testimony by a representative of the mark-holder that the mark appears on every good produced; *Foote*, 413 F.3d at 1248, *aff'g* 238 F. Supp. 2d at 1279; a magazine showing the genuine trademarked goods for sale at the time of offense, *Guerra*, 293 F.3d at 1291; or a civil complaint from a civil action alleging that the victim used the mark before the criminal offense in conjunction with testimony that the trademark owners had protected their marks during the criminal offense, *United States v. Park*, 164 Fed. Appx. 584, 585-86 (9th Cir. 2006).

Although § 2320(f)(1)(A)(ii) does not specify when the registered mark must have been "in use," courts have held that it must have been in use during the defendant's alleged offense. *See Park*, 164 Fed. Appx. at 585 (stating that "registration and use at the time of [a trademark] conspiracy can

be indirectly established if the government provides evidence that trademarks for the relevant items were registered and used prior to and after the conspiracy was formed, as long as the evidence of preceding and subsequent registration and use is reasonably close to the time of the actual conspiracy"); *Foote,* 238 F. Supp. 2d at 1278 n.8 (holding that without a temporal limit "the statute would allow a prosecution for trafficking in products with trademarks that the trademark owner did not begin to use until trial"); *Guerra*, 293 F.3d at 1291. The government should prove that the victim used his genuine mark as early as when the defendant first used his counterfeit mark, if not earlier, and that the victim continued using the genuine mark throughout the offense. *Foote*, 238 F. Supp. 2d at 1274 n.4, 1277-79. Proving that the mark was in use at the time of trial may not suffice to prove that it was in use during the offense. *Id.* at 1278.

e. Use of the Counterfeit Mark "On or In Connection With" Goods or Services

For cases involving goods or services under 18 U.S.C. § 2320(a)(1), the government must prove that the defendant used the counterfeit mark "on or in connection with" goods or services. Similarly, in proving that a good or service is a "counterfeit military good or service" for offenses involving military counterfeits charged under § 2320(a)(3), the government must prove that the good or service "uses a counterfeit mark on or in connection with such good or service." 18 U.S.C. § 2320(f)(4).

In a case involving labels or packaging under 18 U.S.C. § 2320(a)(2), as of the 2006 amendments, the government must show that the counterfeit mark "is applied to" a label, documentation, packaging, or the like that is "designed, marketed, or otherwise intended to be used *on or in connection with* the goods or services for which the mark is registered." § 2320(f)(1)(A)(iii) (emphasis added). The 2006 amendments addressing labels also recognized that a counterfeit mark might not just be applied to or used in connection with labels, documentation, and packaging, but might even "consist[] of" a label, documentation, or packaging component, as was discussed in *United States v. Giles*, 213 F.3d 1247, 1252 n.7 (10th Cir. 2000). See Section B.3.c. of this Chapter.

The term "in connection with" has a broader meaning than "on." For example, a defendant who uses a counterfeit mark to advertise a name-brand good or service and then provides an unmarked, off-brand or no-brand good or service can be said to have used a counterfeit mark "in connection with" the

good or service, even if he did not use it "on" the good or service. This conduct should therefore be covered by § 2320.

Even before the 2006 amendments addressing counterfeit labeling, a person who trafficked in labels, documentation, or packaging—unattached to the underlying goods—may have been prosecuted under a theory of conspiracy or aiding-and-abetting a substantive counterfeit goods offense. See Section B.3.c. of this Chapter. The 2006 amendments, however, allow such a defendant to be charged under § 2320 directly and without resort to theories of secondary liability and in cases where the defendant acted alone. Now, the government need only show that the labels, documentation, or packaging were "designed, marketed, or otherwise intended to be used on or in connection with the goods or services." § 2320(f)(1)(A)(iii).

Because the statute does not define what constitutes "use" of a counterfeit mark by a defendant, defendants may argue that this term should be given a restrictive meaning that does not reach their activities. The Third Circuit rejected this kind of challenge in *United States v. Diallo*, 575 F.3d 252 (3d Cir. 2009). In *Diallo*, law enforcement conducted a traffic stop and found counterfeit Louis Vuitton handbags sealed in plastic bags in the defendant's vehicle. *Id.* at 253-54. Citing *Bailey v. United States*, 514 U.S. 137 (1995), a Supreme Court opinion interpreting the meaning of "uses" in the context of a firearms statute, the defendant asserted that "use" of the counterfeit mark "require[s] active employment of the mark by showing or displaying the goods" bearing that mark. *Diallo*, 575 F.3d at 254. The Third Circuit disagreed, noting that Congress intended to "reach[] a stream of illegal commerce [in counterfeit items] and not simply its point of sale." *Id.* at 260. The court concluded that "use" should be given its "ordinary and natural meaning"; the defendant therefore could be said to have "used" the Louis Vuitton mark because possession of the handbags bearing the counterfeit mark "enabled him to represent to others - falsely - that he owned genuine Louis Vuitton handbags" and to enjoy having such bags in his store's inventory, even if they had not yet been offered for sale. *Id.* at 260-61.

f. The Counterfeit Mark Must Have Been Used for the Same Class of Goods or Services for Which the Genuine Mark Was Registered

Section 2320's definition of a "counterfeit mark" requires the government to show that the defendant's mark is "used in connection with trafficking in any goods [or] services," "identical with, or substantially indistinguishable

from, a mark registered on the principal register in the [USPTO]," and "used in connection with the goods or services for which the mark is registered with the [USPTO]." 18 U.S.C. § 2320(f)(1)(A)(i)-(iii) (but see Section D.8. of this Chapter concerning cases involving Olympic symbols). Congress intended this requirement to be an important and explicit distinction between criminal and civil trademark infringement cases. "[A] plaintiff with a Federal registration for ... [a mark] on typewriters might have a [civil] Lanham Act remedy against a defendant who used that mark to identify typing paper, even though the plaintiff had not registered that mark for use in connection with typing paper. Under [§ 2320], however, the use of the mark ... on typing paper would not count as the use of a 'counterfeit mark.'" *Joint Statement*, 130 Cong. Rec. 31,676 (1984). Prosecutors therefore should be careful to ensure that the class of goods and services in which the defendant trafficked match the class of goods and services for which the victim's mark was registered.

But what about when the defendant uses the mark on *labels, documentation, or packaging* that are for—but unattached to—the class of goods or services indicated on the registration certificate, and not directly on the underlying goods or services themselves? The 2006 amendments addressed this issue by amending § 2320 to allow the prosecution of traffickers in counterfeit labels, documentation, and packaging directly under § 2320. See Section B.3.c. of this Chapter for a discussion of the 2006 amendments and *United States v. Giles*, 213 F.3d 1247, 1253 (10th Cir. 2000). In doing so, Congress did not relax the requirement of matching the defendant's goods and services to the class of goods and services on the registration certificate. Instead, Congress adapted the requirement for labels, documentation, and packaging cases so that the government must prove that those items were "designed, marketed, or otherwise intended to be used on or in connection with the goods or services for which the mark is registered in the United States Patent and Trademark Office." § 2320(f)(1)(A)(iii).

The class of goods or services for which a particular mark was registered can be found on the mark's registration certificate. For information on obtaining these certificates, see Section B.4.c. of this Chapter.

g. Likelihood of Confusion, Mistake, or Deception

The government must prove that the counterfeit mark is "likely to cause confusion, to cause mistake, or to deceive." 18 U.S.C. § 2320(f)(1)(A)(iv). (For the standards in cases involving protected Olympic symbols, see Section

D.8. of this Chapter.) Because this requirement is included in the definition of a "counterfeit mark," it is not necessary for prosecutors to separately charge that the counterfeit mark is "likely to cause confusion, to cause mistake, or to deceive" in the indictment, particularly with respect to charges under 18 U.S.C. § 2320(a)(1) and (3). Prosecutors may, however, want to consider including the language when charging trafficking in labeling components in violation of 18 U.S.C. § 2320(a)(2), because that subsection expressly incorporates the language "likely to cause confusion, to cause mistake, or to deceive" in the statutory provision. Although courts and commentators routinely focus only on the counterfeit mark's propensity to confuse, the statute also allows for proof of mistake or deception, and all three should be charged in the indictment.

The government does not have to prove that the defendant's conduct resulted in actual confusion because "[t]he statute expressly requires only *likelihood* of confusion." *United States v. Yamin*, 868 F.2d 130, 133 (5th Cir. 1989) (emphasis added).

Defendants often argue that their conduct raised no likelihood of confusion because the purchaser knew that the goods were counterfeit, for example because the fake goods were offered at an unusually low price, or because the defendant specifically told the purchaser that the goods were counterfeit. Courts have uniformly rejected these arguments under the theory of "secondary" or "post-sale" confusion (i.e., the confusion of the direct purchaser's downstream customers or even of non-purchasers who could be confused by seeing the counterfeit merchandise on the street). *See, e.g.*, *United States v. Foote*, 413 F.3d 1240, 1245-6 (10th Cir. 2005); *United States v. Hon*, 904 F.2d 803, 808 (2d Cir. 1990); *Yamin*, 868 F.2d at 133; *United States v. Torkington*, 812 F.2d 1347, 1352 (11th Cir. 1987)*; United States v. Gantos*, 817 F.2d 41, 43 (8th Cir. 1987); *United States v. Gonzales*, 630 F. Supp. 894, 896 (S.D. Fla. 1986) (denying motion to dismiss § 2320 indictment because defendants' low price did not preclude finding that they could cause confusion, mistake or deception). For example, in *Foote*, the defendant argued that because he "openly advertised that he sold counterfeit merchandise" and "informed each customer that his merchandise was fake," his actions did not meet the confusion requirement in § 2320. *Foote*, 413 F.3d at 1245. The Tenth Circuit rejected this argument because the confusion requirement is "not restricted to instances in which direct purchasers are confused or deceived by the counterfeit goods." *Id.* (internal quotation marks omitted) (citing *Yamin*, 868 F.2d at 132). Rather, the plain language of the statute indicates that it is "the defendant's use of the product

in commerce (i.e., the sale of the counterfeit product) that is likely to cause confusion, mistake, or deception in the public in general." *Foote*, 413 F.3d at 1246; *see also Torkington,* 812 F.2d at 1353 ("A trademark holder's ability to use its mark to symbolize its reputation is harmed when *potential* purchasers of its goods see unauthentic goods and identify these goods with the trademark holder.") (emphasis added) (citations omitted); S. Rep. No. 98-526 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3627.

The post-sale confusion doctrine was originally developed by courts in interpreting the identical confusion provision in the Lanham Act. *See* 4 J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* § 23:7 (4th ed. 2012). Courts adopted the doctrine in criminal cases because to hold otherwise would undermine the goals of trademark protection. Section 2320 was "not just designed for the protection of consumers," but also for "the protection of trademarks themselves and for the prevention of the cheapening and dilution of the genuine product." *Hon*, 904 F.2d at 806; *see also Torkington,* 812 F.2d at 1352-53; Stop Counterfeiting in Manufactured Goods Act, H. R. Rep. 109-68, at 8 n.2 (2005), *reprinted in* 2006 U.S.C.C.A.N. 211, 216 ("Congress was concerned not only that trademark counterfeiting defrauds purchasers, ... but also that counterfeiters can earn enormous profits by capitalizing on the ... efforts of honest manufacturers at little expense to themselves.") (citations, alterations in original, and internal quotation marks omitted). The Second Circuit interpreted "section 2320's confusion requirement to include the non-purchasing public advances the important purpose underlying the trademark laws of protecting the trademark owner's investment in the quality of the mark and his product's reputation, one that is independent of the goal of preventing consumer deception." *Hon*, 904 F.2d at 806; *see also United States v. Farmer*, 370 F.3d 435, 441 (4th Cir. 2004) (Congress intended to give trademark owners "the 'right to control the quality of the goods manufactured and sold' under that trademark") (citations omitted). This is the same reason why the government need not demonstrate that the counterfeit product is of lesser quality than the genuine product. *E.g.*, *Farmer*, 370 F.3d at 441. Even if the consumer is not defrauded, the counterfeiter is still trading off another's name without authorization. See Section D.1. of this Chapter.

Because the government need only prove the likelihood of confusion, it need not prove that the defendant intended to defraud or mislead purchasers. *See United States v. Brooks*, 111 F.3d 365, 372 (4th Cir. 1997) (rejecting defense that defendants did not use counterfeit marks "for the purpose of deception

or to cause confusion or mistake"); *Yamin*, 868 F.2d at 132 (holding that the statute's application is not restricted to instances in which direct purchasers are confused or deceived by the counterfeit goods); *Gantos*, 817 F.2d at 42-43 (affirming conviction even though defendant disclosed to his immediate customers that Rolex watches were copies); *Torkington,* 812 F.2d at 1353 n.7 (noting that Congress eliminated from § 2320 a *mens rea* element consisting of an intent to deceive or defraud).

Likelihood of confusion can be proved with a variety of evidence, such as the testimony of customers who mistakenly bought fakes, experts on market confusion, or victim representatives who can discuss the fake and real goods' similarities. *See, e.g.*, 4 J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* §§ 23:2, 13, 17, 63 (4th ed. 2012); *see also United States v. Penton*, 303 Fed. Appx. 774, 781-82 (11th Cir. 2008). Although evidence of actual confusion is not necessary, it can often be very persuasive. *See United States v. McEvoy*, 820 F.2d 1170, 1172 (11th Cir. 1987) (affirming conviction based on, *inter alia,* expert testimony that customers often confuse fake and genuine watches and on a defense witness's inability to distinguish between fake and genuine watches).

It is worth noting that in civil counterfeiting cases, where two marks are identical or substantially indistinguishable and are used on the same good, confusion is presumed. *E.g.*, *Polo Fashions, Inc. v. Craftex, Inc.*, 816 F.2d 145, 148 (4th Cir. 1987) ("Where, as here, one produces counterfeit goods in an apparent attempt to capitalize upon the popularity of, and demand for, another's product, there is a presumption of a likelihood of confusion."). In such civil counterfeiting cases, federal courts do not consider the "*Polaroid*" factors set forth in *Polaroid Corp. v. Polarad Elecs. Corp.*, 287 F.2d 492, 495 (2d Cir. 1961), commonly associated with civil trademark infringement cases. *Id.* (test used in civil cases to determine likelihood of confusion unless goods are identical and directly competitive); *Colgate-Palmolive v. J.M.D. All-Star Import and Export Inc.*, 486 F. Supp. 2d 286, 289 (S.D.N.Y. 2007) ("When counterfeit marks are involved, it is not necessary to consider the factors set out in *Polaroid* [], which are used to determine whether a mark is a colorable imitation of a registered mark that creates a likelihood of confusion about it source, because counterfeit marks are inherently confusing.") (internal quotation marks and citations omitted).

Unlike civil counterfeit trademark law, and as already noted, § 2320(f)'s definition of "counterfeit mark" expressly requires the government to prove

likelihood of confusion in a criminal counterfeiting case. Congress included this requirement "to ensure that no conduct will be criminalized by this act that does not constitute trademark infringement under the Lanham Act." *Joint Statement*, 130 Cong. Rec. 31,675 (1984). Nevertheless, prosecutors should resist defendants' attempts to require the government to prove the civil *Polaroid* factors to determine likelihood of confusion because of the heightened requirements already imposed by the other elements of § 2320. Where those heightened elements are met, likelihood of confusion is all but certain. For instance, the government can only bring a case under § 2320 where the class of goods are identical. *See* § 2320(f)(1)(A)(i)-(iii). Section 2320's definition of a "counterfeit mark" requires the government to show that the defendant's mark is "used in connection with trafficking in any goods [or] services," "identical with, or substantially indistinguishable from, a mark registered on the principal register in the [USPTO]," and "used in connection with the goods or services for which the mark is registered with the [USPTO]." *Id.* In other words, the government already must meet a requirement not present in civil counterfeiting cases – that a defendant used their counterfeit mark on the same class of goods on which the trademark owners use their genuine, federally registered marks. "Where the products are identical and the jury has concluded that the defendant has met the two-pronged *mens rea* standard of section 2320, a requirement that confusion among actual or potential purchasers be shown is unnecessary." *United States v. Hon*, 904 F.2d 803, 808 (2d Cir. 1990); *United States v. Torkington*, 812 F.3d 1347, 1351 n.4 (11th Cir. 1987) (the likelihood of confusion "*element should be easily satisfied if the other elements of a 'counterfeit mark' have been proven – since a counterfeit mark is the most egregious example of a mark that is likely to cause confusion*") (quoting *Joint Statement*, 130 Cong. Rec. 31,675 (1984)) (emphasis in original).

For the same reasons, prosecutors should also oppose attempts to compel courts to incorporate the "*Polaroid* factors" in jury instructions regarding § 2320's likelihood of confusion requirement. *Hon*, 904 F.2d at 808, 809 (rejecting defendant's appeal for failure to instruct on *Polaroid* factors because "the non-exclusive *Polaroid* factors themselves ... are designed to assess infringement '[w]here the products are different'" and that "[a] defendant is not entitled to a jury charge simply to create a reasonable doubt when on the facts and the law as correctly applied there should be none") (quoting *Polaroid*, 287 F.2d at 495); *United States v. McEvoy*, 820 F.2d 1170, 1172, 1172 n.1 (11th Cir. 1987) (rejecting appeal for failure to "give an instruction which listed factors to be considered in determining" likelihood of confusion and expressing "no

opinion as to whether the district court would have abused its discretion if it had given the requested instruction"). In any event, criminal jury instructions need not set forth the *Polaroid* multi-factor test because it is not contained in the statute. *See McEvoy*, 820 F.2d at 1172.

As to how the comparison should be made between the counterfeit and legitimate products at trial, civil law suggests three principles. First, counterfeit and genuine marks should "be compared in their entireties" and "should not be dissected or split up into [] component parts [with] each part then compared with corresponding parts" because "[i]t is the impression that the mark as a whole creates on the average reasonably prudent buyer and not the parts thereof, that is important." 4 J. Thomas McCarthy, *McCarthy on Trademarks* § 23:41 (4th ed. 2012) (footnote omitted); *see also id.* § 23:42. Second, because the average purchaser focuses on two marks' similarities rather than their differences, the fact finder should do the same. *Id.* § 23:41. Third, whether the counterfeit and genuine marks should be compared side by side or serially depends on how the average consumer would encounter them in the market: "Where products in the relevant market are not typically displayed in the same locations, centering on whether they are likely to be distinguished when viewed simultaneously is incorrect, and will result in a faulty likelihood-of-confusion analysis." *Louis Vuitton Malletier v. Burlington Coat Factory Warehouse Corp.*, 426 F.3d 532, 534 (2d Cir. 2005) (Calabresi, J.) (discussing likelihood of confusing handbags); *see also* 4 *McCarthy on Trademarks* § 23:58-59. *But see Louis Vuitton Malletier v. Dooney & Bourke, Inc.*, 454 F.3d 108, 117 (2d Cir. 2006) (suggesting that side-by-side comparison may be acceptable to determine whether goods are identical). Finally, in a criminal case, even if some of the markings on the defendant's goods deviate from those on the original and his goods are of noticeably poor quality, they are counterfeit so long as his goods bear at least one trademark identical to or substantially indistinguishable from the original. *See United States v. Yi*, 460 F.3d 623, 627 n.1, 629 n.4, 637 n.14 (5th Cir. 2006).

5. The Defendant Used the Counterfeit Mark "Knowingly"

The final element required for a § 2320 offense is that the defendant "knowingly" used the counterfeit mark on or in connection with the trafficked goods or services. In cases involving labels, documentation, or packaging, the government must prove that the defendant trafficked in such items "knowing that a counterfeit mark has been applied thereto, the use of which is likely to cause confusion, to cause mistake, or to deceive." § 2320(a) (as amended by the

Stop Counterfeiting in Manufactured Goods Act, Pub L. No. 109-181, § 1, 120 Stat. 285 (2006)).

To prove this element, the government must present evidence that the defendant had "an awareness or a firm belief" that the mark used was counterfeit. *See Joint Statement*, 130 Cong. Rec. 31,674 (1984).

Knowledge can also be proved with evidence that the defendant acted with willful blindness, conscious avoidance, or deliberate ignorance, which means the defendant "deliberately closed his eyes to what otherwise would have been obvious to him concerning the fact in question." *See United States v. Brodie*, 403 F.3d 123, 132 (3d Cir. 2005) (quotation and citation omitted). "[I]f the prosecution proves that the defendant was 'willfully blind' to the counterfeit nature of the mark, it will have met its burden of showing 'knowledge.'" *Joint Statement*, 130 Cong. Rec. 31,674 (1984) (citing *United States v. Jewell*, 532 F.2d 697 (9th Cir. 1976) (other citations omitted)); *see also United States v. Hiltz*, 14 Fed. Appx. 17, 19 (1st Cir. 2001); *United States v. Hamamoto*, No. 99-10019, 2000 WL 1036199, *2 (9th Cir. July 27, 2000); *cf.* Tal S. Benschar et al., *Proving Willfulness in Trademark Counterfeiting Cases*, 27 Colum. J.L. & Arts 121, 125 (2003). Although certain circuits may be generally reticent to allow proof of willful blindness to satisfy actual knowledge in criminal cases, Congress's specific intent with respect to § 2320(a) should trump that reluctance in these cases.

On the other hand, "a manufacturer who believes in good faith that he or she has a prior right to use a particular mark, or that a mark does not infringe a registered mark, could not be said to 'know' that the mark is counterfeit." *Joint Statement*, 130 Cong. Rec. 31,674 (1984).

The government may prove the defendant's knowledge or willful blindness of a counterfeit mark through direct or circumstantial evidence. Circumstantial evidence could include evidence that:

- the defendant purchased or sold goods after notice of potential infringement;
- the defendant knew that the victim distributed its goods only through authorized dealers, when the defendant and his supplier were not authorized dealers;
- the goods came from a questionable supplier;
- the defendant or his source used coded invoices for branded merchandise;

- the goods were of inferior quality; or
- the goods were bought or sold for an unusually low price.

Cf. Tal S. Benschar et al., *Proving Willfulness in Trademark Counterfeiting Cases*, 27 Colum. J.L. & Arts 121, 130-35 (2003) (discussing civil cases).

For more case examples, see *United States v. Lam*, 677 F.3d 190, 200 n.10 (4th Cir. 2012) (finding that "[t]he government presented ample evidence at trial to allow a reasonable jury to conclude that Appellants were aware that the marks on their handbags and wallets were counterfeit, including evidence of: their use of multiple shell companies and multiple ports to import the counterfeit goods, the manner in which they transported and concealed the counterfeit merchandise, the civil lawsuit Burberry instituted against them, and the multiple seizure notices they received from CBP"); *United States v. Barry*, 390 Fed. Appx. 949, 950-51 (11th Cir. 2010) (per curiam); *United States v. Garrison*, 380 Fed. Appx. 423, 426 (5th Cir. 2010) (per curiam) (sufficient evidence of deliberate indifference existed where defendant was previously notified that the merchandise he was selling was counterfeit, he knew he did not have necessary license to sell trademarked merchandise, and cost of merchandise was very low); *United States v. Hatem Abu Hassan*, 280 Fed. Appx. 271, 274 (4th Cir. 2008) (per curiam) (defendant knew pills sold to an undercover officer were counterfeit because defendant assured the undercover officer the pills were "effective" and provided the undercover officer with a free sample of the pills, the packaging of the counterfeit pills did not indicate their source, and defendant had an "abundant supply" of the pills); *United States v. George*, 233 Fed. Appx. 402, 404-05 (5th Cir. 2007) (per curiam) (evidence was sufficient to prove willful blindness where, *inter alia*, licensed pharmacist knew prices he was paying for drugs were far below market rate and he failed to inquire about the legitimacy of the medication); *United States v. Park*, 164 Fed. Appx. 584, 585-86 (9th Cir. 2006) (holding that government demonstrated knowing use of a counterfeit mark by introducing settlement agreement from an earlier civil action between defendant and victim in which she had agreed not to sell identical merchandise with which she was caught in criminal case) (unpublished); *United States v. Yi*, 460 F.3d 623, 629-30 (5th Cir. 2006) (jury could conclude that defendant knew the marks were counterfeit, notwithstanding his numerous factual counterarguments, in light of the defendant's admissions, attempt to bribe a Customs agent, receipt of cease-and-desist letters, and the counterfeit goods' poor quality); *United States v. Guerra*, 293 F.3d 1279, 1287-88 (11th Cir. 2002) (citing defendant's knowledge that

the counterfeit labels he produced were not all being sold to authorized dealers of Cuban cigars and that the purchasers of defendant's counterfeit labels did not purport to be authorized dealers themselves); *United States v. Jewell*, 532 F.2d 697, 699-702 (9th Cir. 1976) (upholding willful blindness instruction when defendant had declined to buy drugs from a stranger but then agreed to drive the stranger's car from Mexico to the United States for $100, while he suspected there was something wrong or illegal with the car and examined the car but avoided investigating an apparently hidden compartment in the trunk that was later found to contain drugs) (cited in § 2320's legislative history); *United States v. Hamamoto*, No. 99-10019, 2000 WL 1036199, at *1 (9th Cir. July 27, 2000) (reasoning that knowledge element satisfied by evidence that defendant, a customs agent in Guam, received bribes to clear airway bills for goods imported from Korea, a primary source of counterfeit goods to Guam); *United States v. Sung*, 51 F.3d 92, 93-94 (7th Cir. 1995) (holding that although the victim's genuine mark was not always identified with the ® symbol, defendant's knowledge that the "marks were on the bottles, caps, and boxes" of the counterfeit shampoo he sold sufficed because § 2320(f)(1)(A)(ii) imposes on the defendant "the duty to inquire about the status of the mark"); *United States v. Rodriguez*, Nos. 88-1125, 88-1127, 1989 WL 69934, at *2 (9th Cir. June 23, 1989) (citing defendant's own distinction between "phony" and "real" Rolex watches, defendant's inability to sell the counterfeits at work, and defendant's admission that she had to be quiet about selling them); *United States v. McEvoy*, 820 F.2d 1170, 1172-73 (11th Cir. 1987) (rejecting defendants' contention that § 2320 was unconstitutionally vague because defendants appeared to know "that their actions in selling the watches violated the law," particularly when defendants admitted that the watches seized by the government contained trademarks virtually identical to registered trademarks for Rolex, Piaget, and Gucci).

For a case in which circumstantial evidence was insufficient, consider *United States v. Sultan*, 115 F.3d 321 (5th Cir. 1997). In *Sultan,* the defendant shared a warehouse with an auto parts dealer who obtained re-manufactured auto parts and altered them to make them look new. *Id.* at 323-24. Although the two businesses were kept separate, the defendant purchased a large amount of merchandise from the auto parts dealer. *Id.* at 324. In holding that the government failed to show that the defendant knew that he was selling counterfeit parts, the Fifth Circuit largely rejected the government's circumstantial evidence of knowledge, including:

- The defendant's penchant for thriftiness and knowledge of market prices. *Id.* at 326.
- The defendant's inconsistent statements to investigators (because he may have made these statements for non-criminal reasons). *Id.*
- The defendant shared the warehouse space with the auto parts dealer (which alone was not sufficient because the defendant's mere presence in a climate of criminal activity could not serve as a basis for conviction). *Id.* at 328.
- The counterfeit parts' low prices (which alone were not sufficient evidence of knowledge when there were legal ways to obtain goods at this price range and the defendant was paying 80% to 90% of the market price for legitimate distributors). *Id.* at 329.
- Evidence of the defendant's knowledge regarding legitimate packaging (because there was no evidence that the defendant was aware that the packaging materials stored by the auto parts dealer were counterfeit, particularly when one witness never saw the defendant in the counterfeit room and another witness testified that the defendant kept his inventory separate from the auto parts dealer). *Id.* at 329-30.

Holding that this circumstantial evidence required the jury to go "beyond making reasonable inferences" by "making unreasonable leaps," the court reversed the conviction on the ground that there was insufficient evidence to support the jury's finding that the defendant knowingly used a counterfeit mark beyond a reasonable doubt. *Id.* at 330.

The government need not prove that the defendant knew that the mark he counterfeited was registered with the United States Patent and Trademark Office. See Section B.4.c. of this Chapter. Nor must the government prove that the defendant knew that his conduct constituted a crime. *Hamling v. United States,* 418 U.S. 87, 123 (1974)*; United States v. Baker*, 807 F.2d 427, 428-30 (5th Cir. 1986); *United States v. Yu Chunchai*, No. 10-50540, 2012 WL 1332404, at *1 (9th Cir. Apr. 18, 2012) (unpublished) ("The statute does not require that the government prove that the defendant knew that his conduct was illegal ...."). And at least one unpublished Ninth Circuit opinion has held that the government need not prove that the defendant "knew that the mark was likely to cause confusion." *Yu Chunchai*, 2012 WL 1332404, at *1.

Finally, in *Lam*, the Fourth Circuit held that defendants waived their right to raise for the first time on appeal a sufficiency challenge to a jury's finding that defendants knowingly used a counterfeit mark where defendants failed

to raise that challenge in an earlier Rule 29(c) motion raising other specific grounds for challenging their § 2320 conviction. 677 F.3d at 200.

6. Trafficking in Counterfeit Military Goods or Services

The National Defense Authorization Act for FY 2012 ("NDAA"), Pub. L. No. 112-81, 125 Stat. 1298 (2011), amended § 2320 to create a new offense for trafficking in "counterfeit military goods or services." Specifically, the new offense provides enhanced criminal penalties for anyone who:

> traffics in goods or services knowing that such good or service is a counterfeit military good or service the use, malfunction, or failure of which is likely to cause serious bodily injury or death, the disclosure of classified information, impairment of combat operations, or other significant harm to a combat operation, a member of the Armed Forces, or to national security....

18 U.S.C. § 2320(a)(3). The amendments also define the new term "counterfeit military good or service":

> the term "counterfeit military good or service" means a good or service that uses a counterfeit mark on or in connection with such good or service and that—
> (A) is falsely identified or labeled as meeting military specifications, or
> (B) is intended for use in a military or national security application...

18 U.S.C. § 2320(f)(4).

Although the new "counterfeit military good" offense is located in a separate subsection (§ 2320(a)(3)) from the preexisting counterfeit goods offense (§ 2320(a)(1)), a charge under the "counterfeit military" provision will require proving essentially all the same elements of a traditional counterfeit goods charge under § 2320(a)(1), plus several additional elements. That is, a § 2320(a)(3) charge requires that the defendant "traffic" in "goods or services," and must act "knowing[ly]," just as in § 2320(a)(1). Whereas § 2320(a)(1) requires that the defendant "knowingly use a counterfeit mark on or in connection with such good or service," § 2320(a)(3) requires that the defendant act "knowing that such good or service is a counterfeit military good or service." A "counterfeit military good or service" is defined as a good or service "that uses a counterfeit mark on or in connection with such good or service," as well as meeting certain other criteria. 18 U.S.C. § 2320(f)(4).

The counterfeit military good or service offense can thus be thought of as an enhancement of the traditional § 2320(a)(1) "counterfeit goods" charge, where certain additional elements are met. Some of those elements are set forth in the definition of "counterfeit military good or service," while other elements are included in the offense language in § 2320(a)(3).

a. "Counterfeit Military Good or Service"

As noted above, to qualify as a "counterfeit military good or service" the good or service must "use[] a counterfeit mark on or in connection with such good or service." 18 U.S.C. § 2320(f)(4). In addition, the good or service must also be *either* (A) falsely identified or labeled as meeting military specifications, or (B) intended for use in a military or national security application.

To date no courts have had the opportunity to interpret the meaning of "counterfeit military good or service" in § 2320 and there is minimal legislative history regarding the specific language of the NDAA amendments to § 2320. The plain language of the statutory definition, however, indicates that to prove a violation of the "counterfeit military good or service" provision, the government will need to show either that the defendant knew the goods (or services) in question were falsely identified as meeting a military specification (such as a consumer semiconductor chip that is falsely represented or labeled as being a military grade chip), or alternatively, that the defendant intended that the goods or services be used in a military or national security application, or at least knew that the goods or services in which the defendants were trafficking were intended by others (e.g., the ultimate purchasers) for use in a military or national security application.

Issues involving counterfeit parts in the military supply chain, which prompted the NDAA amendments, have been the subject of investigation by several government and Congressional bodies. *See, e.g.*, U.S. Gov't Accountability Office, GAO-12-375, *Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms* (2012), *available at* http://gao.gov/products/GAO-12-375 and GAO-10-389; U.S. Gov't Accountability Office, GAO-10-389, *DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts* (2010), *available at* http://www.gao.gov/products/GAO-10-389; U.S. Dep't of Commerce, *Defense Industrial Base Assessment: Counterfeit Electronics* (2010), *available at* http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf; S. Rep. No. 112-167 (2012) (Report of the Senate

Committee on Armed Services); *The Committee's Investigation Into Counterfeit Electronic Parts in the Department of Defense Supply Chain: Hearing Before the Senate Committee on Armed Services*, 112th Cong. (2011), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112shrg72702/pdf/CHRG-112shrg72702.pdf.

b. "Use, Malfunction, or Failure" is Likely to Cause Specified Harms

To prove an offense under 18 U.S.C. § 2320(a)(3), the government must also demonstrate "the use, malfunction, or failure of [the counterfeit military good or service] is likely to cause" one of several specified harms:

1. serious bodily injury or death;
2. the disclosure of classified information;
3. impairment of combat operations, or;
4. other significant harm to a combat operation, a member of the Armed Forces, or to national security.

Note that the government need not prove that such harms actually occurred, or that the use or failure of a counterfeit would necessarily cause one of the specified harms, but only that such harm would be "likely" to occur.

7. Trafficking in Counterfeit Drugs

The Food and Drug Administration Safety and Innovation Act ("FDASIA"), Pub. L. No. 112-144, 126 Stat. 993 (2012) amended § 2320 to create a new offense for trafficking in "counterfeit" drugs. The amendments increase the criminal penalties for anyone who "traffics in a counterfeit drug." 18 U.S.C. § 2320(a)(4).

The amendments also create a new definition for the term "counterfeit drug":

> the term "counterfeit drug" means a drug, as defined by section 201 of the Federal Food, Drug, and Cosmetic Act, that uses a counterfeit mark on or in connection with the drug.

18 U.S.C. § 2320(f)(6). The term "drug" is defined by reference to the definition used in the Food, Drug, and Cosmetic Act (FDCA), 21 U.S.C. § 321(g)(1). The FDCA broadly defines the term "drug" to include any articles recognized in official formularies or pharmacopoeia (§ 321(g)(1)(A)), any articles intended for use to treat or prevent disease (§ 321(g)(1)(B)), or any articles intended to affect the structure or any function of human or animal

bodies (§ 321(g)(1)(C)), but generally does not include dietary supplements or food (§ 321(g)(1)(C)-(D)). Note that although 21 U.S.C. § 321(g) includes its own definition of "counterfeit drug" (*see* § 321(g)(2)),—the FDASIA's new definition of "counterfeit drug" in 18 U.S.C. § 2320(f)(6) governs cases charged under § 2320(a)(4).

As explained previously in Section B.1. of this Chapter, with respect to the new "counterfeit drug" offense, § 2320(a)(4), Congress failed to include the *mens rea* requirement—which exists for § 2320(a)(1)-(3)—that the government must prove that the defendant *knowingly* used a counterfeit mark. As of this writing, Congress has not yet amended this provision to correct the omission. However, in order to prove a charge under § 2320(a)(4), it is recommended that prosecutors prove the same elements of a traditional counterfeit goods charge under § 2320(a)(1) plus additional elements set forth in the definition of "counterfeit drug." A "counterfeit drug" is defined as a drug, as defined by the FDCA in 21 U.S.C. § 321(g)(1), that "uses a counterfeit mark on or in connection with the drug." 18 U.S.C. § 2320(f)(6). Just as the "counterfeit military good" offense discussed in the previous subsection, the counterfeit drug offense can be thought of as an enhancement of the traditional § 2320(a)(1) "counterfeit goods" charge.

8. Venue

Venue is proper in any state through which counterfeit goods travel after the defendant obtains control over the goods. *See United States v. DeFreitas*, 92 F. Supp. 2d 272 (S.D.N.Y. 2000). In *DeFreitas*, the defendant imported counterfeit Beanie Babies from China to New Jersey via New York for eventual sale in New Jersey. *Id*. at 276. The defendant challenged his conviction under §§ 2320 and 371 (conspiracy) on the basis of improper venue in New York, arguing that the substantive offense under § 2320 did not begin until he received the counterfeit goods in New Jersey. The court rejected his argument by holding that trafficking is a continuing offense beginning with obtaining control over the counterfeit goods, continuing with transport, and ending with the transfer or disposal of the goods. *Id.* at 277. Because the offense began when the defendant purchased the counterfeit goods in China and directed that they be shipped to New Jersey, venue was proper at any point through which the goods traveled after they entered the United States, including the Southern District of New York. *Id*.

C. Defenses

Many general defenses, such as the absence of proper venue or jurisdiction, are available in every criminal case and their application needs no further elaboration here. The following discussion addresses defenses specific to § 2320.

1. Authorized-Use Defense: Overrun Goods

The authorized-use defense excludes from the definition of counterfeit mark any mark that is

> used in connection with goods or services[, or a mark or designation applied to labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature used in connection with such goods or services,] of which the manufacturer or producer was, at the time of the manufacture or production in question[,] authorized to use the mark or designation for the type of goods or services so manufactured or produced, by the holder of the right to use such mark or designation.

18 U.S.C. § 2320(f)(1)(B). The bracketed language was inserted by the Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1(b)(3), 120 Stat. 285, 287 (2006), and thus applies only to offenses arising after that time.

The authorized-use defense applies to "overrun" goods or services, that is, goods or services that an otherwise authorized manufacturer or producer makes and sells on the side without the mark-holder or licensor's knowledge or approval. For instance, consider a trademark licensee who is authorized to make 500,000 umbrellas bearing the licensor's trademark but who manufactures without authorization an additional 500,000 umbrellas bearing that mark during the course of the license. *Joint Statement*, 130 Cong. Rec. 31,676 (1984). Because the trademark owner in this situation can protect himself through "contractual and other civil remedies," Congress felt that it was "inappropriate to criminalize such practices." *Id.* Thus, "[i]f a licensee manufactures overruns during the course of the valid license, the marks on those goods will remain noncounterfeit for purposes of this act." *Id.*

The overrun goods defense attaches to the overrun goods themselves, not just to the party who produced them. This follows from § 2320(f)(1)(B)'s specification that overrun goods are not counterfeit. Consequently, any overrun goods that are produced and completed during the course of the license remain noncounterfeit even after the license runs out, *Joint Statement*, 130 Cong. Rec. 31,676 (1984), and the defense is available to any party who traffics in overrun goods downstream of the manufacturer. The legislative history behind §2320(f)(1)(B) shows Congress' intent that the overrun goods defense be an affirmative defense; "the burden [is] on the defendant to prove that the goods or services in question fall within the overrun exclusion." *Joint Statement*, 130 Cong. Rec. 31,676 (1984).

The overrun goods defense does not, however, allow counterfeiters to escape criminal liability by attaching real or overrun labels to counterfeits. As discussed in Section B.4.a. of this Chapter (citing 4 *McCarthy on Trademarks and Unfair Competition* § 25:15 (4th ed. 2012) and *United States v. Petrosian*,126 F.3d 1232, 1234 (9th Cir. 1997)), it is standard trademark law—both civil and criminal—that a genuine or authentic mark becomes counterfeit when it is used in connection with something else that is counterfeit. As revised, the authorized-use exception provides that a counterfeit mark "does not include any mark or designation *used in connection with goods or services*, or a mark or designation applied to labels, ... documentation, or packaging of any type or nature *used in connection with such goods or services*, of which the manufacturer or producer was, at the time of the manufacture or production in question, authorized to use the mark or designation for the type of goods or services so manufactured or produced, by the holder of the right to use such mark or designation." 18 U.S.C. § 2320(f)(1)(B) (emphasis added) (numbered § 2320(e)(1) prior to Dec. 31, 2011). The 2006 amendments reworded the authorized-use exception to retain its focus on whether the goods and services are overrun, rather than whether the labels, documentation, or packaging themselves are overrun. As before, the text focuses on the authorization of the manufacturer or producer *of the goods and services*, not the manufacturer or producer *of the labels, documentation, or packaging*. Interpreting the amendment differently would cause a major change in trademark law, one which Congress would have signaled in much clearer terms had the change been intended. Given that the 2006 amendments were intended to strengthen the government's ability to prosecute cases concerning counterfeit labels, documentation, and packaging, and the legislative history indicates nothing to the contrary, the authorized-use exception should still allow the government to prosecute those

who use or traffic in real or overrun labels, documentation, or packaging to turn inauthentic goods into counterfeits.

The overrun defense does have a few limitations. First, "the overrun exemption does not apply if a licensee produces a type of goods in connection with which he or she was not authorized to use the trademark in question." *Joint Statement*, 130 Cong. Rec. 31,676-77 (1984). For example, "if a licensee is authorized to produce 'Zephyr' trench coats, but without permission manufactures 'Zephyr' wallets, the overrun exception would not apply." *Id*. at 31,677. In this example, the licensee could be prosecuted for producing the wallets only if the 'Zephyr' mark was registered for use on wallets as well as trench coats. See also Section B.4.f. of this Chapter.

Second, the overrun goods defense is limited to goods or services for which authorization existed "during the *entire* period of production or manufacture." *United States v. Bohai Trading Co.*, 45 F.3d 577, 580 (1st Cir. 1995). In *Bohai*, Stride Rite authorized the defendant to arrange for the manufacture of 200,000 pairs of its KEDS trademarked sneakers in China in 1987 and 1988. *Id.* at 578. Stride Rite terminated the defendant's license in the spring of 1989, after which the defendant arranged for the Chinese factory to manufacture an additional 100,000 pairs of KEDS and to backdate the shoes as being produced in 1988. *Id.* at 578-79. The defendant then imported the shoes to the United States and sold them as genuine KEDS. *Id.* at 579. On appeal from its conviction, the defendant argued that § 2320 was unconstitutionally vague because it did not define the meaning of "production" within the authorized-use exception, and thus the defendant could not discern whether its conduct was illegal. The First Circuit disagreed, holding that the statute's plain language clearly indicates that the licensee must have a valid trademark license at all stages of manufacture or production. *Id.* at 580-81. Stride Rite's permission to assemble materials and train Chinese factory workers in 1988 (which the defendant argued was "production" within the meaning of § 2320) did not authorize him to apply the KEDS trademark to shoes in 1989 after his license was terminated. *Id.*

The use of a licensee's rejected irregular goods was addressed in *United States v. Farmer*, 370 F.3d 435 (4th Cir. 2004). In *Farmer*, the defendant purchased irregular garments without trademarks from legitimate manufacturers' authorized factories, and had different companies sew or silk-screen on the manufacturers' trademarks. *Id.* at 437-38. On appeal, the defendant argued that he had not "confuse[d] customers about the source of his goods" because the garments had been manufactured to the trademark holders' specifications

by factories from which the trademark holders themselves purchased. *Id.* at 440. The Fourth Circuit disagreed, reasoning that § 2320 focuses not on the quality of the counterfeit goods but on the counterfeit trademark attached to those goods and the right of trademark holders to control the manufacturing and sale of goods with their trademarks. *Id*. at 440-41. Although the decision did not specifically discuss the overrun goods defense, that defense likely would have been rejected because the garments had not been fully manufactured or produced until the marks were placed on them by the companies the defendant hired, which were not authorized by the trademark holders. Had the defendant instead purchased garments from authorized factories with the trademarks already on them, the overrun goods defense might have prevailed.

The defendant bears the burden of proving "that the goods or services in question fall within the overrun exclusion, under both the criminal and civil provisions" by a preponderance of the evidence. *Joint Statement*, 130 Cong. Rec. 31,676 (1984).

2. Authorized-Use Defense: Gray Market Goods

"Gray market goods," also known as "parallel imports," are "trademarked goods legitimately manufactured and sold overseas, and then imported into the United States" through channels outside the trademark owner's traditional distribution channels. *Joint Statement*, 130 Cong. Rec. 31,676 (1984) (citing *Bell & Howell: Mamiya Co. v. Masel Supply Co.*, 719 F.2d 42 (2d Cir. 1983)). As with overrun goods, the marks on gray market goods are placed there with the mark-holder's authorization. What the mark-holder has not authorized is the sale of those foreign goods within the United States.

Just as with overrun goods (discussed in Section C.1 of this Chapter), the authorized-use defense excludes parallel imports and gray market goods from the definition of a counterfeit mark because such a mark is "placed there with the consent of the trademark owner." *Joint Statement*, 130 Cong. Rec. 31,676 (1984). Congress carefully considered "gray market" goods and intended that those who traffic in them not be prosecuted. *Id.*; S. Rep. No. 98-526, at 11 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3627, 3637.

Additionally, as with the overrun goods defense, the gray market goods defense is available not just to the party who produced the goods, but also to any party who traffics in them downstream, because § 2320(f)(1) (numbered § 2320(e)(1) prior to Dec. 31, 2011) declares that such goods are not counterfeit. Although there are no reported decisions directly on point, it is

unlikely that a court would interpret the gray market or parallel import defense to be an affirmative defense. First, Congress drew a distinction between these defenses in the legislative history. While the legislative history makes clear that overrun goods are exempt from the definition of counterfeit by § 2320(f)(1) and that the defendant bears the burden of proving the goods at issue are overrun, *Joint Statement*, 130 Cong. Rec. 31,676 (1984), the *Joint Statement* makes no such statement about gray market goods. Furthermore, the *Joint Statement* expressly stated that the bill's sponsors did not consider gray market and parallel import goods to meet the definition of counterfeit marks, because the marks were placed on the goods with the consent of the trademark owner or a person affiliated with the trademark owner. *Id*.

This defense does not apply if the gray market goods were subsequently modified or remarked in a manner that made the new mark counterfeit. See Section C.3. of this Chapter.

3. Repackaging Genuine Goods

When the defendant's goods themselves are genuine and bear the trademark of the rights-holder but have been repackaged by the defendant, whether the defendant's repackaging is criminal depends on whether he deceived the public or damaged the mark-owner's good will. This rule ran through the cases, and was written into § 2320 by the Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1, 120 Stat. 285 (2006).

United States v. Hanafy held that a defendant cannot be prosecuted under § 2320 for repackaging genuine goods with reproduced trademarks if the defendant did so without deceiving or confusing others. 302 F.3d 485 (5th Cir. 2002). In *Hanafy*, the defendants purchased individual cans of infant formula from various convenience stores and other sources and then repackaged the cans into trays for resale. *Id*. at 486. The defendants marked the shipping trays with reproductions of the can manufacturers' trademarks and resold the trays to other wholesalers. *Id.* Although the cans had not been packaged by the original manufacturers for resale in this form, the defendants' goods were genuine, unadulterated, and were sold within the "sell by" date. *Id.* The district court ruled that the unauthorized use of a reproduction of a mark in connection with genuine goods (that is, what the mark represents the goods to be) does not violate § 2320. *Id.* at 487-88. In so ruling, the court concluded that the repackaging rule of *Prestonettes, Inc. v. Coty*, 264 U.S. 359, 368-69 (1924),

which applies to actions brought under the Lanham Act, does not apply to criminal prosecutions under § 2320. *Hanafy*, 302 F.3d at 488.

Affirming the district court, the Fifth Circuit held that the shipping trays did not qualify as counterfeit under § 2320. *Id*. at 488-89. Although repackaging the goods without the manufacturer's approval or control might violate civil trademark law, attaching a mark to trays containing the "genuine unadulterated, unexpired products associated with that mark does not give rise to criminal liability under section 2320." *Id.* at 489. The court distinguished *Petrosian*, which involved fake Coca-Cola in real Coke bottles, because the infant formula in this case was genuine. *Id.* See also the discussion of *Petrosian* in Section B.4.a. of this Chapter. Thus, under *Hanafy*, a person usually cannot be prosecuted under § 2320 for repackaging goods with reproductions of the original trademark if the goods themselves are genuine and in the same condition that they would have been had the rights-holder distributed them itself.

United States v. Milstein, 401 F.3d 53, 62-63 (2d Cir. 2005), confirmed that a defendant can be prosecuted under § 2320 if he repackages genuine goods to defraud consumers, such as by presenting fraudulent information. In *Milstein*, the defendant obtained drugs manufactured for foreign markets and repackaged them with false lot numbers and other markings to make the drugs appear as if they had been approved by the FDA for sale in the United States. 401 F.3d at 59-60. The repackaged drugs were not identical to the drugs manufactured for U.S. markets. *Id*. On appeal, the defendant cited *Hanafy* to argue that his repackaging did not violate § 2320. *Id*. at 62. The Second Circuit distinguished *Hanafy* because "[w]hile the cans in *Hanafy* were 'merely being repackaged, such that consumers could be sure of the goods' quality and source,' ... the drugs here were repackaged so that consumers would believe foreign versions of the drug were in fact domestic, FDA-approved versions." *Id.* (quoting *United States v. Farmer*, 370 F.3d 435, 441 n.1 (4th Cir. 2004) (citing *Hanafy*, 302 F.3d at 486)). The critical distinction was that *Hanafy*'s false marks "contained no more information than that which was carried on the cans themselves," whereas "Milstein sold [drugs] in forged packaging bearing false lot numbers." *Id.* (internal quotation marks and alterations omitted). *See also United States v. Lexington Wholesale Co.*, 71 Fed. Appx. 507, 508 (6th Cir. 2003) (affirming restitution for a § 2320 conviction based on repackaging of loose cans of infant formula into cases that did not accurately reflect the "use by" date).

In amending § 2320 in 2006, Congress essentially codified *Hanafy* and *Milstein* in a new subsection of § 2320: "Nothing in this section shall entitle the United States to bring a criminal cause of action under this section for the repackaging of genuine goods or services not intended to deceive or confuse." 18 U.S.C. § 2320(g) (previously numbered as § 2320(f)). With respect to *Hanafy*, the legislative history explains that "[b]ecause the bill amends the definition of a counterfeit trademark to include packaging and labeling formats, which can be used lawfully by a variety of businesses, this language is intended to clarify that repackaging activities such as combining single genuine products into gift sets, separating combination sets of genuine goods into individual items for resale, inserting coupons into original packaging or repackaged items, affixing labels to track or otherwise identify genuine products, [and] removing genuine goods from original packaging for customized retail displays are not intended to be prosecuted as counterfeiting activities under the amended title 18 U.S.C. § 2320." H.R. Rep. No. 109-68, at 8 & n.1 (2005).

Congress also intended to codify the *Milstein* rule to allow prosecution of those who repackage genuine goods in a manner that defrauds consumers. In determining whether to prosecute such a case, the government is expected to "consider evidence tending to show an intent to deceive or confuse such as altering, concealing, or obliterating expiration dates, or information important to the consumer['s] use of the product such as safety and health information about the quality, performance, or use of the product or service; statements or other markings that a used, discarded, or refurbished product is new; or statements or other markings that the product meets testing and certification requirements." *Id.* "Also relevant ... would be a meaningful variance from product testing and certification requirements, placing seals on product containers that have been opened and the original manufacturer's seal has been broken, or altering or otherwise adulterating the genuine product." *Id.* at 9.

Although *Hanafy* and *Milstein* concern consumables such as food and drugs, similar issues arise in other industries. *See, e.g.*, *Intel Corp. v. Terabyte Int'l, Inc.*, 6 F.3d 614, 616, 620 (9th Cir. 1993) (holding defendants liable for infringement for purchasing and later distributing computer chips from a distributor who had relabeled the chips with a model number signifying a higher processing speed); *Adobe Sys. Inc. v. One Stop Micro, Inc.*, 84 F. Supp. 2d 1086, 1088 (N.D. Cal. 2000) (holding defendants liable for infringement for sale of educational versions adulterated and repackaged as full retail versions).

Section 2320(g) does not preempt the prosecution of deceptionless repackaging under statutes other than § 2320: "Nothing in this section shall entitle the United States to bring a criminal cause of action *under this section* for the repackaging of genuine goods or services not intended to deceive or confuse." 18 U.S.C. § 2320(g) (emphasis added). For instance, repackaging cases that involve consumer products such as food, drugs, medical devices, cosmetics, and other items designed for consumers to use in the household, might be prosecuted under the product tampering statute, 18 U.S.C. § 1365, which addresses tampering with labels and communicating false information that a consumer product was tainted, or under the Food, Drug, and Cosmetic Act, 21 U.S.C. §§ 331(a), 333, 343, 352, 362, which punishes trafficking in misbranded food, drugs and cosmetics. See Section F. of this Chapter.

4. Lanham Act Defenses

The Lanham Act's civil defenses have been incorporated as defenses against criminal charges brought under § 2320 to the extent applicable. "All defenses, affirmative defenses, and limitations on remedies that would be applicable in an action under the Lanham Act [for trademark infringement] shall be applicable in a prosecution under this section." 18 U.S.C. § 2320(d) (previously numbered § 2320(c) prior to Dec. 31, 2011); *see also Joint Statement,* 130 Cong. Rec. 31,675 (1984)("only those defenses, affirmative defenses, and limitations on relief [in the Lanham Act] that are relevant under the circumstances will be applicable"). In addition, "any affirmative defense under the Lanham Act will remain an affirmative defense under this [section], which a defendant must prove by a preponderance of the evidence." *Id*.

Statutory defenses under the Lanham Act primarily address the incontestability of a mark once it has been registered for five years. 15 U.S.C. § 1115(b). The defenses to incontestability include: 1) fraud by the mark-holder in obtaining the registration; 2) abandonment of the mark by its owner; 3) the registered mark's use by or with the registrant to misrepresent the source of the goods or services on or in connection with which the mark is used; 4) use of the name, term, or device charged to be an infringement is a use of the defendant's individual name in his own business, or of someone in privity with that party, or a term that is used in good faith to describe the goods or services of such party or their geographic origin; 5) innocent and continuous prior use of the mark without registration by the defendant; 6) the defendant's innocent prior use of the mark with registration; 7) use by the mark-holder of a trademark in violation of the antitrust laws; 8) the mark is functional; and

9) equitable defenses, such as laches, estoppel, and acquiescence. *Id.* Other Lanham Act defenses or limitations mentioned prominently in the legislative history are those limitations on actions against printers and newspapers in 15 U.S.C. § 1114(2). For instance, the owner of an infringed mark is limited to an injunction against future printing under 15 U.S.C. § 1125(a). *See* 15 U.S.C. § 1114(2)(A); *Joint Statement*, 130 Cong. Rec. 31,675 (1984). For an extensive discussion of these defenses, see David J. Goldstone & Peter J. Toren, *The Criminalization of Trademark Counterfeiting*, 31 Conn. L. Rev. 1, 43-65 (1998).

The applicability of the Lanham Act's statute of limitations (or lack thereof) is discussed in Section C.5. of this Chapter.

Civil cases decided under the Lanham Act may prove instructive when applying the Lanham Act defenses in criminal cases, but those defenses should not be applied mechanically in a criminal case. For example, although an "unclean hands" defense may deny relief to a plaintiff mark-holder in a civil case, 15 U.S.C. § 1115(b)(3), (9); 37 C.F.R. § 2.114(b)(1) (2012), the mark-holder's unclean hands are less relevant in a criminal case. This is because the mark-holder is not a party and the prosecutors act in the public's interest rather than exclusively the mark-holder's interest. Thus, application of this Lanham Act defense in a criminal case might not serve the public interest.

At this writing, few criminal cases address the Lanham Act defenses. *See, e.g.*, *United States v. Milstein,* 401 F.3d 53, 63-64 (2d Cir. 2005) (holding laches defense unavailable in § 2320 prosecutions); *United States v. Sung*, 51 F.3d 92, 94 (7th Cir. 1995) (discussing how 15 U.S.C. § 1111's limitations on remedies in civil cases applies to criminal cases); *United States v. Sheng*, No. 92-10631, 1994 WL 198626 (9th Cir. 1994) (affirming denial of defendant's motion for discovery concerning antitrust defense, due to defendant's failure to make a *prima facie* case for discovery); *United States v. Shinyder,* No. 88-7236, 1989 WL 126528 (4th Cir. 1989) (per curiam) (holding that defendant failed to demonstrate ineffective assistance of counsel because defendant gave his attorney no information regarding purported invalidity of victim's mark due to its prior use by defendant); *United States v. Almany,* 872 F.2d 924 (9th Cir. 1989) (appeal based on evidentiary issues related to Lanham Act defenses).

5. Statute of Limitations

Under 18 U.S.C. § 3282(a), the statute of limitations for almost all non-capital federal crimes is five years unless otherwise expressly provided by law.

Because § 2320 does not specify a limitations period itself, violations of § 2320 are subject to the general five-year limitations period. *See United States v. Foote,* 413 F.3d 1240, 1247 (10th Cir. 2005); *United States v. Milstein*, No. CR 96-899 (RJD), 2000 WL 516784, at *1 (E.D.N.Y. 2000).

Defendants, however, sometimes seek a shorter statute of limitations by arguing that the courts should apply the limitations period applicable to civil trademark violations. In *Foote*, for instance, the defendant argued that the statute of limitations should be determined by state law because § 2320(d) incorporates "[a]ll defenses, affirmative defenses, and limitations on remedies that would be applicable under the Lanham Act," and courts apply state statutes of limitations to Lanham Act cases since the federal civil statute does not contain an express limitation period. *Foote*, 413 F.3d at 1247. The Tenth Circuit disagreed, holding that the lack of an "express statute of limitations in either the Counterfeit Trademark Act or the Lanham Act" means that the general criminal limitations period in § 3282(a) applies. *Id.*; *see also United States v. Foote,* 238 F. Supp. 2d 1271, 1276-77 (D. Kan. 2002) (containing an extended policy discussion of this issue).

6. Vagueness Challenges

Courts have rejected challenges to § 2320 under the Fifth Amendment on vagueness grounds. A statute can be struck down as unconstitutionally vague if it either (1) fails to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits, or (2) authorizes or encourages arbitrary and discriminatory enforcement. *City of Chicago v. Morales*, 527 U.S. 41, 56 (1999). Federal courts have uniformly rejected challenges to various terms within § 2320 as unconstitutionally vague. *E.g.*, *United States v. McEvoy*, 820 F.2d 1170 (11th Cir. 1987) (rejecting claim that the Trademark Counterfeiting Act, 18 U.S.C. § 2320, is unconstitutionally vague on its face); *United States v. Lam*, 677 F.3d 190, 201-03 (4th Cir. 2012) (rejecting vagueness claim based on § 2320's use of the phrase "substantially indistinguishable"); *United States v. Bohai Trading Co.*, 45 F.3d 577 (1st Cir. 1995) (rejecting vagueness claim based on § 2320's use of the phrase "at the time of the manufacture or production" in its "authorized-use" exception); *United States v. Hon*, 904 F.2d 803 (2d Cir. 1990) (rejecting claim that § 2320 is unconstitutionally vague as applied to "likelihood of confusion" jury charge); *United States v. Diallo*, 476 F. Supp. 2d 497 (W.D. Pa. 2007) (rejecting vagueness claim based on Congress' decision not to define the term "use" in § 2320), *aff'd*, 575 F.3d 252 (3d Cir.), *cert. denied*, 130 S. Ct. 813 (2009).

D. Special Issues

1. High-Quality and Low-Quality Counterfeits

Defense counsel often argue that it is inappropriate to charge a § 2320 offense if the counterfeit goods are of very low or, conversely, very high quality, arguing that nobody is fooled by low-quality counterfeits and that nobody is harmed or deceived by high-quality counterfeits. Both arguments are misguided. *See, e.g.*, *United States v. Farmer*, 370 F.3d 435 (4th Cir. 2004) (affirming conviction under § 2320 for irregular garments purchased from factories that manufactured garments to trademark holder's specifications); *United States v. Gonzalez*, 630 F. Supp. 894, 896 (S.D. Fla.1986) (denying motion to dismiss § 2320 indictment because the counterfeits' low price did not preclude finding that they could cause confusion, mistake or deception).

The government's response lies in the plain language of the statute. Subsections 2320(a) and (f) focus on whether the counterfeit mark is likely to cause confusion, cause mistake, or to deceive and make no mention of the counterfeit item's quality. *See United States v. Foote*, 413 F.3d 1240, 1246 (10th Cir. 2005) ("[T]he correct test is whether the defendant's use of the mark was likely to cause confusion, mistake or deception in the public in general."). As discussed in Section B.4.g. of this Chapter, § 2320 was "not just designed for the protection of consumers," but also for "the protection of trademarks themselves and for the prevention of the cheapening and dilution of the genuine product." *United States v. Hon*, 904 F.2d 803, 806 (2d Cir. 1990) (internal quotation marks and citations omitted). In this vein, "[o]ne of the rights that a trademark confers upon its owner is the 'right to control the quality of the goods manufactured and sold' under that trademark. *For this purpose the actual quality of the goods is irrelevant; it is the control of quality that a trademark holder is entitled to maintain.*" *Farmer*, 370 F.3d at 441 (internal quotation marks and citations omitted) (emphasis added). "When courts find that selling an item at an excessively cheap price precludes a finding that such an item is 'counterfeit' under 18 U.S.C. § 2320[] in that the use of the goods is not likely to cause confusion, to cause mistake, or to deceive, they are, in effect, thwarting the purposes behind such legislation." *Gonzalez*, 630 F. Supp. at 896; *United States v. Torkington*, 812 F.2d 1347, 1350 n.3 (11th Cir. 1987) (holding that *Gonzalez* "adopted essentially the same interpretation that we do here").

Because both high-quality and low-quality counterfeit goods affect the intellectual property rights of the trademark holder, a § 2320 charge can be appropriate in either circumstance. See also Section B.4.g. of this Chapter.

2. Counterfeit Goods with Genuine Trademarks

Although the definition of "counterfeit mark" in § 2320(f) indicates that the mark itself must be counterfeit, not the good to which it is attached, a genuine or authentic mark becomes counterfeit when it is applied to counterfeit goods. See the discussion of *United States v. Petrosian*, 126 F.3d 1232 (9th Cir. 1997), in Section B.4.a. of this Chapter.

Genuine trademarks can also become counterfeit when they are applied to genuine product in a manner that misrepresents the genuine product's quality. See Section C.3. of this Chapter.

3. Selling Fakes While Admitting That They Are Fakes

Defendants who disclose to consumers that their merchandise is counterfeit may not argue successfully that no criminal liability should attach because their customers were not deceived into thinking they were purchasing genuine goods. See Section B.4.g. of this Chapter.

4. Selling Another's Trademarked Goods As One's Own (Reverse Passing-Off)

Agents sometimes inquire whether a target can be prosecuted for criminal trademark infringement if he sells another's goods as his own under his own trademark, such as selling stolen Marlboro cigarettes as his own Acme brand cigarettes. This conduct, called "reverse passing-off," is civilly actionable under the Lanham Act. *See, e.g.*, *Dastar Corp. v. 20th Century Fox Film Corp.*, 539 U.S. 23, 32-37 (2003); *Web Printing Controls Co. v. Oxy-Dry Corp.,* 906 F.2d 1202 (7th Cir. 1990); *Arrow United Indus., Inc. v. Hugh Richards, Inc.,* 678 F.2d 410, 416 (2d Cir. 1982); *Smith v. Montoro,* 648 F.2d 602, 606 & n.5 (9th Cir. 1981). Reverse passing-off is not a crime under § 2320, however, because it does not involve the use of a counterfeit mark as defined in § 2320(f). In the example above, the defendant's own Acme mark would be, in fact, a genuine mark.

5. Mark-Holder's Failure to Use ® Symbol

The trademark code requires the holder of a federally registered mark to give others notice of registration by displaying the mark with the words "Registered in U.S. Patent and Trademark Office," "Re. U.S. Pat. & Tm. Off.," or the familiar ® symbol. Without this notice next to its mark on its goods and services, the mark-holder cannot recover its profits or damages against an infringer unless the infringer had actual notice of the registration. 15 U.S.C. § 1111. The commonly-seen ™ and ℠ symbols do *not* give notice of federal registration; they can be used with unregistered marks. 3 J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* § 19:148 (4th ed. 2012).

The victim's intentional or inadvertent failure to use the statutory means of notice mentioned above does not preclude the defendant's prosecution under § 2320. *United States v. Sung*, 51 F.3d 92, 93-94 (7th Cir. 1995). Section 2320 criminalizes counterfeiting "whether or not the defendant knew [the victim's] mark was so registered." 18 U.S.C. § 2320(f)(1)(A)(ii); *Sung*, 51 F.3d at 93-94. Moreover, the notice provisions in 15 U.S.C. § 1111 do not create a defense that excuses infringement, but rather they only limit the mark-holder's remedies. *Sung*, 51 F.3d at 94; *see also* 3 *McCarthy on Trademarks and Unfair Competition* § 19:144 ("Failure to use the statutory symbol does not create a defense: it is merely a limitation on remedies.") (footnote omitted). For a discussion of how these remedies are limited in criminal cases, see Section E.3. of this Chapter.

6. Storage Costs and Destruction

Unlike many other intellectual property crimes, criminal trademark infringement frequently generates a substantial quantity of physical evidence. Although large intellectual property seizures can be a problem to store, storage is the safest option. (Chapter X of this Manual discusses whether victims may assist with storage.) If storage is not feasible, part of the evidence probably can be destroyed after a hearing if the seized property is counterfeit. Destruction of the evidence, however, carries its own complications with respect to making evidence available for defendants and jurors to inspect and employing sound procedures for taking representative samples.

The decision to allege all or only a part of the seized intellectual property in the indictment and at trial must be made on a case-by-case basis. In most cases, it should be possible either to indict for all seized goods and present

evidence of a representative sample to prove the whole at trial, or to indict and present evidence of only some of the goods, using evidence of the full quantity as relevant conduct only at sentencing. (Chapter VIII's discussion of determining the infringement amount considers the justification for and methods of estimation.) Charging a subset for trial and proving the remainder at sentencing may also have some tactical advantages, such as streamlining the trial and deferring loss calculations to the sentencing phase.

Because these issues can become quite complex, prosecutors should consider them early on, even before the search is conducted. If the prosecutor wants all the evidence to be available for trial, it is important to coordinate with the seizing agency to ensure that any forfeited material is not destroyed or is at least destroyed only after a sound procedure for taking representative samples is completed. (Of course, destruction is not permissible until the items have been forfeited.)

Prosecutors can discuss these issues with the Computer Crime and Intellectual Property Section at (202) 514-1026.

7. Units of Prosecution

Because a defendant often traffics in numerous counterfeit trademarks, drafting an indictment that reflects the defendant's actions is not always easy. The United States Department of Justice's *Criminal Resource Manual* 215, *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00215.htm, advises that "all United States Attorneys should charge in indictments and informations as few separate counts as are reasonably necessary to prosecute fully and successfully and to provide for a fair sentence on conviction"; it also generally recommends charging no more than fifteen counts. But trademark counterfeiters of any significant size will often have infringed numerous trademarks in numerous transactions.

The charging determination in a trademark counterfeiting case, as in other criminal cases, is subject to the rule of reason, and generally the best approach is to organize charges around specific courses of conduct in order to keep the case as straightforward as possible for the jury. Counts may be organized by the mark infringed; the identity of the mark-holder; or the date upon which the infringing goods were obtained, manufactured, distributed, or seized. Indictments charging counterfeiting schemes can be unified through a conspiracy count.

If the defendant infringed only one trademark, the defendant can be charged with a single count. Separate sales of goods bearing the same counterfeit mark, however, have sometimes been charged in separate counts. *See, e.g.*, *United States v. Gantos*, 817 F.2d 41, 42 (8th Cir. 1987) (defendant charged and convicted on four counts, each for separate sales of counterfeit Rolex watches).

If the defendant counterfeited multiple marks, the indictment may also contain separate counts for each separate genuine mark. For example, in *United States v. Song*, 934 F.2d 105 (7th Cir. 1991), the court upheld the defendant's conviction on five separate counts "because she was trafficking in goods bearing five different counterfeit marks." *Id.* at 109. The court relied on the plain language of § 2320, which punishes someone who "'intentionally traffics or attempts to traffic in goods or services *and knowingly uses a counterfeit mark*' on such goods or services." *Id*. at 108 (quoting the then-current version of 18 U.S.C. § 2320(a)) (emphasis in original) (footnote omitted).

The courts have not yet addressed several charging issues that will continue to arise in trademark prosecutions:

- Whether a single sale of multiple items that infringe multiple trademarks may be charged in a single counterfeiting count. The issue is whether such a charge would be duplicitous—i.e., charging two or more distinct offenses in a single count—or rather just an allegation that multiple means were used to commit a single offense. Prosecutors who confront this issue should consult the Department's manual, Office of Legal Education, U.S. Dep't of Justice, *Federal Grand Jury Practice* § 11.30 (2008) (concerning duplicitous indictments), *available at* http://dojnet.doj.gov/usao/eousa/ole/usabook/gjma/11gjma.htm#11.30.
- How multiple counterfeit trademarks on a single good should be charged in a criminal indictment: as one count, using the counterfeit good as the unit of prosecution, or as multiple counts, using each mark as a unit of prosecution.
- Whether a defendant who traffics in a counterfeit good wrapped in counterfeit packaging may be charged in one count that covers both the good and packaging and/or whether charging the good and packaging separately in multiple counts is necessary or permissible, now that § 2320 (as amended 2006) criminalizes trafficking in counterfeit labels, documentation, and packaging in addition to counterfeit goods and services.

8. Olympic Symbols

The definition of "counterfeit mark" in § 2320(f)(1)(B) includes designations protected by the Olympic Charter Act, such as the five interlocking rings of the Olympic games. *See also* 36 U.S.C. § 220506(a)(2) (giving the United States Olympic Committee exclusive rights to the symbol of the International Olympic Committee, consisting of 5 interlocking rings, the symbol of the International Paralympic Committee, consisting of 3 TaiGeuks, and the symbol of the Pan-American Sports Organization, consisting of a torch surrounded by concentric rings).

Some of the rules that apply to prosecutions involving other marks do not apply to cases involving the Olympic symbols:

- The mark need not have been registered on the principal register in the USPTO. Section 2320(f)(1)(A)'s registration requirements do not apply to cases dealing with criminal trademark infringement of Olympic symbols. *Compare* 18 U.S.C. § 2320(f)(1)(A)(ii) *with* § 2320(f)(1)(B); *see also* 36 U.S.C. § 220506; *Joint Statement*, 130 Cong. Rec. 31,675 (1984) (explicitly exempting cases involving Olympic symbols from the registration requirement). See also the discussion of registration in Section B.4.c. of this Chapter.
- Section 2320(f)(1)(A)(ii)'s use requirement does not apply to cases involving protected Olympic symbols. See also the discussion of use in Section B.4.d. of this Chapter.
- The requirement that the defendant have used the counterfeit mark in connection with the goods or services for which the mark had been registered does not apply to cases involving protected Olympic symbols. See also Section B.4.f. of this Chapter.
- In cases involving protected Olympic symbols, the mark is counterfeit under 18 U.S.C. § 2320(f)(1)(B) if the defendant's counterfeit symbols are "identical with, or substantially indistinguishable" from the genuine symbols. No further proof of likely confusion, mistake, or deception is required. See also Section B.4.g. of this Chapter.

The other rules discussed in this Chapter apply equally to cases involving Olympic symbols.

E. Penalties

1. Fines and Imprisonment

For violations of § 2320(a)(1) (goods or services) or (a)(2) (labels, etc.), the maximum penalty for a first offense is up to 10 years imprisonment and a $2 million fine for an individual defendant and up to $5 million for organizational defendants. 18 U.S.C. § 2320(b)(1)(A). Subsequent offenses are subject to penalties of up to 20 years imprisonment and a $5 million fine for an individual defendant and up to $15 million for organizational defendants. *Id.* § 2320(b)(1)(B).

For violations of § 2320(a)(3) and (a)(4), involving counterfeit military goods or services and counterfeit drugs, respectively, the maximum penalty is imprisonment up to 20 years and a fine of up to $5 million for individuals and up to $15 million for organizational defendants. *Id.* § 2320(b)(3)(A). Subsequent offenses are subject to up to 30 years imprisonment and a $15 million fine for individuals and up to $30 million fine for organizational defendants. *Id.* § 2320(b)(3)(B).

If a defendant knowingly or recklessly causes or attempts to cause serious bodily harm or death by any of the offenses listed in subsection 2320(a), enhanced penalties may be available under § 2320(b)(2). In the case of serious bodily injury the statutory penalty is up to 20 years' imprisonment and a $5 million fine for an individual and up to $15 million for an organizational defendant. The fines are the same in the case of death, however, an individual is subject to life imprisonment. *Id.* § 2320(b)(2)(A), (B).

A challenge to incarceration, probation, and supervised release, on the ground that these remedies are not present in the civil Lanham Act, was rejected in *United States v. Foote*, No. CR.A. 00-20091-01-KHV, 2003 WL 22466158, at *2-3 (D. Kan. July 31, 2003), *aff'd in part on other grounds*, 413 F.3d 1240 (10th Cir. 2005).

2. Restitution

The 2006 amendments to § 2320 expressly provided for restitution to victims of trademark counterfeiting. The amendments codified the prior practice in which restitution was awarded under 18 U.S.C. § 3663A(c)(1)(A)(ii), which provides mandatory restitution to victims of crimes against property in Title 18, and under Section 5E1.1 of the Sentencing Guidelines,

which provides restitution when there is an identifiable victim and restitution is authorized under 18 U.S.C. § 3663A. *See, e.g.*, *United States v. Lexington,* 71 Fed. Appx. 507, 508 (6th Cir. 2003) (affirming contested restitution order under 18 U.S.C. § 3663 and U.S.S.G. § 5E1.1 following a § 2320 conviction); *United States v. Hanna,* No. 02 CR.1364-01 (RWS), 2003 WL 22705133, at *3 (S.D.N.Y. Nov. 17, 2003) (including restitution in sentence for § 2320 conviction). See also Chapter VIII of this Manual.

The 2008 PRO-IP Act revised § 2320's restitution provision to refer to 18 U.S.C. § 2323, the general forfeiture and restitution provision for IP offenses also created by the PRO-IP Act. Section 2323(c), provides that "[w]hen a person is convicted of an offense under [§ 2320, *inter alia*], the court, pursuant to sections 3556, 3663A, and 3664 of [title 18], shall order the person to pay restitution to any victim of the offense as an offense against property referred to in section 3663A(c)(1)(A)(ii)." 18 U.S.C. § 2320(c). This provision does not mean that restitution will be proper in every § 2320 case, but rather that restitution shall be ordered under 18 U.S.C. § 3663A(c)(1)(A)(ii) if there is a victim who was harmed in a manner that would entitle him to restitution as the victim of a property crime.

Before the 2008 amendments, § 2320 expressly defined the term "victim" as having "the meaning given that term in section 3663A(a)(2)," that is, "a person directly and proximately harmed as a result of the commission of an offense for which restitution may be ordered." *See* § 2320(b)(5) (2008). That express reference to § 3663A(a)(2) was removed when the specific restitution language in § 2320 was replaced with a reference to the IP forfeiture and restitution provision in § 2323 by the PRO-IP Act in 2008. Although § 2323 does not define the term "victim," there is no language in the PRO-IP Act or its legislative history to indicate that Congress intended these amendments to alter the definition of "victim" for § 2320 purposes, or to refer to any definition other than that provided in § 3663A(a)(2). Even under that definition, however, there remains some question whether a mark-holder qualifies for restitution if the defendant's conduct did not diminish the mark-holder's sales. See also Chapter VIII of this Manual.

The restitution amount should be determined by calculating only "the actual amount [of infringing goods] placed into commerce and sold." *United States v. Beydoun*, 469 F.3d 102, 108 (5th Cir. 2006). Although infringing items intended to be sold (but not actually sold) may be included in valuing loss for sentencing purposes, such goods should not be included in calculating

restitution. *Id*. at 107-108. Furthermore, since the purpose of restitution is to compensate victims for actual losses, restitution should be based on the legitimate seller's gross, rather than net, lost profits. *Id.* at 108.

In § 2320 cases, the victim's right to restitution may be subject to an important qualification: the Lanham Act's limitation on remedies in 15 U.S.C. § 1111. In civil cases, 15 U.S.C. § 1111 prohibits a plaintiff from recovering monetary damages from a defendant who lacked actual notice that the plaintiff's mark was registered. One court has ruled that 15 U.S.C. § 1111 limits restitution in a § 2320 prosecution because § 2320 incorporates civil Lanham Act defenses. *United States v. Sung*, 51 F.3d 92, 94 (7th Cir. 1995) ("[R]estitution in a criminal case is the counterpart to damages in civil litigation," and thus "restitution payable to the trademark owner is proper only if the goods contained the proper notice or the infringer had actual knowledge of the registration."). In *Sung*, the Seventh Circuit held that specific findings on these points—proper notice or actual knowledge of the registration—must be made by the sentencing court on the record before ordering restitution. *Id*. See the discussion of what constitutes proper notice in Section D.5. of this Chapter. For cases addressing how to prove notice or the defendant's actual knowledge of registration, see *United Servs. Auto. Ass'n v. Nat'l Car Rental Sys. Inc.*, No. Civ. A.SA00CA1370G, 2001 WL 1910543, at *4 (W.D. Tex. Sept. 26, 2001) (holding that "actual notice requirement is met when a party receives information portraying a registered trademark bearing a ® symbol," including a letter asking the defendant to cease and desist); *Schweitzz Dist. Co. v. P & K Trading Inc.*, No. 93 CV 4785, 1998 WL 472505, at *5 (E.D.N.Y. July 16, 1998) (holding that defendant's testimony that it was aware of plaintiff's use of the ® symbol on the open market sufficed to prove notice).

Even if other courts follow the Seventh Circuit's holding in *Sung*, two points are worth noting. First, the defendant's knowledge or notice of the registration is not a defense to a criminal conviction; it is only a limitation on remedies. *See Sung*, 51 F.3d at 93-94. See also Section D.5. of this Chapter. Second, the rule should not limit restitution to any consumers whom the defendant defrauded. *Sung*'s holding was stated only in terms of restitution to the mark-holder, and its rationale should not be extended to consumers who have no say in whether the mark-holder gave the defendant notice. *See Sung*, 51 F.3d at 94 (noting that "as a form of money damages, restitution [is] *payable to the trademark owner*") (emphasis added); *cf. United States v. Foote*, 413 F.3d 1240, 1252 (10th Cir. 2005) (holding *Sung* inapplicable to criminal fines because

"[t]he court's conclusion in *Sung* was based on its reasoning that restitution is a form of money damages payable to the trademark owner. Unlike restitution [to the trademark owner], fines are a form of criminal punishment rather than a form of damages, and are payable to the government rather than to the trademark owner.") (citation omitted).

For a more in-depth discussion of restitution in intellectual property crimes, such as whether a trademark-holder can be awarded restitution even if the defendant did not cost the trademark-holder any sales, see Chapter VIII of this Manual.

3. Forfeiture

Forfeiture is covered in Chapter VIII of this Manual.

4. Sentencing Guidelines

The applicable sentencing guideline is U.S. Sentencing Guidelines Manual § 2B5.3. It is covered in Chapter VIII of this Manual.

Historically, one of the most difficult issues in sentencing § 2320 offenses concerned how to compute the infringement amount of goods in the defendant's possession to which he had not yet applied a counterfeit mark. In cases where the defendant had not completed applying the counterfeit mark to the goods at issue (such as in cases of attempt or aiding-and-abetting where the defendants produced counterfeit labels or packaging), courts held that the government was required to establish with a "reasonable certainty" that the defendant intended to complete and traffic in those goods. *United States v. Guerra*, 293 F.3d 1279, 1293-94 (11th Cir. 2002) ("There is no support for the proposition that the number of 'infringing items' may be based on the number of seized articles that have the mere *potential* of ultimately forming a component of a finished counterfeit article, without a determination as to the extent to which defendants had a reasonable likelihood of actually completing the goods."); *United States v. Sung*, 51 F.3d 92, 94-96 (7th Cir. 1995) (remanding for resentencing because the district court did not find with reasonable certainty that Sung intended to sell 240,000 counterfeit shampoo bottles where the only evidence of intent was the possession of counterfeit trademarked shipping cartons that could hold 240,000 bottles, and defendant had liquid to fill only 17,600 bottles). Further, if the counterfeit label was not attached to the good, the counterfeit item's value might have been determined by whether the counterfeit label itself has a market value separate from the value of the infringing item for which it was

intended. *Compare United States v. Bao*, 189 F.3d 860, 866-67 (9th Cir. 1999) (holding that the most appropriate retail value to use in sentencing under 18 U.S.C. § 2318 for trafficking in counterfeit computer software manuals was that of the genuine computer manual, not the total software package) *with Guerra*, 293 F.3d at 1292 (distinguishing *Bao* in § 2320 conviction because the cigar labels had no retail value apart from being attached to the cigars).

In response to the 2006 amendments, which expressly addressed counterfeit labeling components, the Sentencing Commission amended the Application Notes to § 2B5.3 to provide that the retail value of the infringed item should be used to determine the infringement amount when the case involves:

> a counterfeit label, patch, sticker, wrapper, badge, emblem, medallion, charm, box, container, can, case, hangtag, documentation, or packaging of any type or nature (I) that has not been affixed to, or does not enclose or accompany a good or service; and (II) which, had it been so used, would appear to a reasonably informed purchaser to be affixed to, enclosing, or accompanying an identifiable, genuine good or service. In such a case, the "infringed item" is the identifiable, genuine good or service.

United States Sentencing Guidelines § 2B5.3 cmt. n.2(A)(vii) (2012) (as amended by Amendment 682, effective September 12, 2006).

On April 10, 2013, the Sentencing Commission promulgated new Guidelines amendments to address the counterfeit military good or service offense in § 2320(a)(3) that was created by the NDAA for FY2012 (enacted Dec. 31, 2011), and the counterfeit drug offense in § 2320(a)(4) that was created by the FDASIA (enacted July 9, 2012). Under these amendments, both types of offenses will generally be subject to a 2-level enhancement, and counterfeit military goods offenses will also be subject to a minimum offense level of 14. Application of these new Guidelines provisions is discussed further in Chapter VIII of this Manual.

F. Other Charges to Consider

When confronted with a case that implicates counterfeit trademarks, service marks, or certification marks, prosecutors may consider the following crimes in addition to or in lieu of § 2320 charges if § 2320's elements cannot be met:

- **Conspiracy and aiding-and-abetting, 18 U.S.C. §§ 2, 371**

  Consider these charges if the defendant only supplied counterfeit labels or packaging that were attached by another person. See Section B.3.c. of this Chapter.

- **Mail and wire fraud, 18 U.S.C. §§ 1341, 1343**

  These charges can be filed if the defendant used the mail (or other interstate carrier) or wires (including the Internet) in a scheme to defraud purchasers, whether direct or indirect purchasers. Mail and wire fraud may be especially appropriate when there are foreign victims and domestic jurisdiction under § 2320 is difficult to establish. *See Pasquantino v. United States*, 544 U.S. 349, 125 S. Ct. 1766 (2005) (affirming wire fraud conviction where victim was the Canadian government); *United States v. Trapilo*, 130 F.3d 547, 552 (2d Cir. 1997) ("The [wire fraud] statute reaches *any* scheme to defraud involving money or property, whether the scheme seeks to undermine a sovereign's right to impose taxes, or involves foreign victims and governments.") (emphasis in original) (citations omitted).

  Mail and wire fraud charges may be available if the defendant told his direct purchasers that his goods were counterfeit, so long as he and his direct purchasers intended to defraud the direct purchasers' customers. If, however, all the participants intended that the goods be sold to the ultimate customers as admitted "replicas," then mail and wire fraud charges will likely be unavailable.

- **Copyright infringement, 17 U.S.C. § 506, 18 U.S.C. § 2319**

  Consider these charges if the underlying goods are not only trademarked or service marked, but also contain copyrighted

contents, such as books, movies, music, or software. See Chapter II of this Manual.

- **Trafficking in counterfeit labels, illicit labels, or counterfeit documentation or packaging, 18 U.S.C. § 2318**

  Consider charging § 2318 if the labels, documentation, or packaging were intended to be used with copyrighted works. See Chapter VI of this Manual.

- **Trafficking in misbranded food, drugs and cosmetics**

  See Food, Drug, and Cosmetic Act and Title 21 provisions, including 21 U.S.C. §§ 331(a) (prohibitions on misbranding), 333 (criminal penalties), 343 (misbranded food), 352 (misbranded drugs and devices), 362 (misbranded cosmetics) and 841(a)(2) (prohibiting distribution of counterfeit controlled substances).

- **Tampering with consumer products, 18 U.S.C. § 1365**

  Tampering with labels and communicating false information that a consumer product has been tainted.

- **Trafficking in mislabeled wool, fur and textile fiber products**

  Title 15 U.S.C. §§ 68a, 68h (prohibiting commercial dealing in misbranded wool products), 69a, 69i (prohibiting commercial dealing in misbranded fur products), 70a, 70i (prohibiting commercial dealing in misbranded textile fiber products).

- **Racketeer Influenced and Corrupt Organizations (RICO), 18 U.S.C. §§ 1961-1968**

  Consider RICO if the intellectual property crimes are committed by organizations. Counterfeit labeling, 18 U.S.C. § 2318; criminal copyright infringement, 18 U.S.C. § 2319; trafficking in recordings of live musical performances, 18 U.S.C. § 2319A; and trademark counterfeiting, 18 U.S.C. § 2320, are all predicate offenses for a racketeering charge under 18 U.S.C. § 1961(1)(B). A RICO charge requires prior approval from the Organized Crime and Gang Section of the Criminal Division (OCGS). *See United States Attorneys' Manual*

(USAM) 9-110.101, 9-110.320. To contact OCGS, call (202) 514-3594.

- **Money laundering, 18 U.S.C. §§ 1956, 1957**

  Section 2320 is a predicate offense for a money laundering charge. 18 U.S.C. § 1956(c)(7)(D). *See, e.g.*, *United States v. Bohai Trading Co.*, 45 F.3d 577, 579 (1st Cir. 1995) (charging § 2320 and § 1957 offenses).

Those seeking additional information on enforcing criminal provisions of the Food, Drug, and Cosmetic Act designed to protect consumers should contact the Justice Department's Consumer Protection Branch at (202) 616-0295.

Congress has also provided civil remedies for violations of its prohibitions on misbranded goods and has established agencies to enforce those laws, such as the Federal Trade Commission and the Food and Drug Administration. Cases appropriate for civil enforcement may be referred to the appropriate agency. The Federal Trade Commission's Marketing Practices Division, which is part of the Consumer Protection Bureau, may be reached at (202) 326-2412. The Federal Trade Commission's website is www.ftc.gov, and their general information telephone number is (202) 326-2222. The Food and Drug Administration's website is www.fda.gov, and they may be reached by telephone at 1-888-INFO-FDA (1-888-463-6332).

IV.
Theft of Commercial Trade Secrets— 18 U.S.C. §§ 1831-1839

A. Introduction

"A trade secret is really just a piece of information (such as a customer list, or a method of production, or a secret formula for a soft drink) that the holder tries to keep secret by executing confidentiality agreements with employees and others and by hiding the information from outsiders by means of fences, safes, encryption, and other means of concealment, so that the only way the secret can be unmasked is by a breach of contract or a tort." *ConFold Pac., Inc. v. Polaris Indus.*, 433 F.3d 952, 959 (7th Cir. 2006) (Posner, J.) (citations omitted). Or, as Judge Posner could have pointed out, it can also be unmasked by a criminal act.

Congress expressly criminalized the theft of trade secrets with passage of the Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489 (1996) (codified at 18 U.S.C. §§ 1831-1839) (EEA). Prior to the EEA, criminal liability for the theft of trade secrets was available indirectly in limited situations: 18 U.S.C. § 1905 for the unauthorized disclosure of government information, including trade secrets, by a government employee; 18 U.S.C. § 2314 for the interstate transportation of stolen property, including trade secrets; and 18 U.S.C. §§ 1341, 1343, and 1346 for the use of mail or wire communications in a fraud scheme to obtain confidential business information in. See Section G. of this Chapter. And while some state laws provided for criminal enforcement of trade secret theft, the legal landscape was far from uniform.

Congress passed the EEA in 1996 "against a backdrop of increasing threats to corporate security and a rising tide of international and domestic economic espionage." *United States v. Hsu*, 155 F.3d 189, 194 (3d Cir. 1998). Congress further recognized that as America continued to transition to a technology and information-based economy, its businesses' confidential information would

become increasingly tied to America's national security. *See* H.R. Rep. No. 104-788, at 4-7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4023-26; *see also id.* at 7 (1996) (noting "the importance of developing a systematic approach to the problem of economic espionage"). Thus, the EEA was intended to bring the legal framework prohibiting the theft of sensitive and proprietary business information in line with the realities of the information age. *See* 142 Cong. Rec. 27111-12 (1996) (Statement of Senator Specter). The statute closed a gap in federal law that made it difficult to prosecute the theft of trade secrets. *Hsu*, 155 F.3d at 194-95; *see also United States v. Yang*, 281 F.3d 534, 543 (6th Cir. 2002) (noting "the purpose of the EEA was to provide a comprehensive tool for law enforcement personnel to use to fight theft of trade secrets"). In recent years, the number of EEA cases has dramatically increased. *See, e.g.*, U.S. Intellectual Property Enforcement Coordinator, *2011 Annual Report on Intellectual Property Enforcement*, at 30-31 (2012); U.S. Dep't of Justice, *PRO IP Act Annual Report FY2011*, at 18-19 (2011); FBI, *PRO IP Act Annual Report FY2011*, at 1 (2011); U.S. Dep't of Justice, *PRO IP Act Annual Report FY2010*, at 16-18 (2010); FBI, *PRO IP Act Annual Report FY2010*, at 1 (2010).

The EEA has undergone two recent amendments. The Theft of Trade Secrets Clarification Act, Pub. L. No. 112-236, § 2, 126 Stat. 1627 (2012) ("2012 amendment"), enacted December 28, 2012, clarified the "interstate commerce" element of 18 U.S.C. § 1832 in response to the Second Circuit's decision in *United States v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012). The Foreign and Economic Espionage Penalty Enhancement Act, Pub. L. No. 112-269, § 3, 126 Stat. 2442 (2013), enacted January 14, 2013, increased the fines available for 18 U.S.C. § 1831 offenses, and directed the United States Sentencing Commission to review the penalties applicable to EEA offenses.

This Chapter considers a number of issues arising under the Economic Espionage Act in depth. A sample indictment and jury instructions appear at Appendix D. In addition to this Chapter, prosecutors may wish to consult the following treatises or law review articles: Uniform Trade Secrets Act § 1 *et seq.* (amended 1985), 14 U.L.A. 438 (1990); Roger M. Milgrim, *Milgrim on Trade Secrets* (2012); Ronald D. Coenen Jr. et al., *Intellectual Property Crimes*, 48 Am. Crim. L. Rev. 849 (2011); 6 Joel Androphy, White Collar Crime, § 45:1-18 (2012); Economic Espionage and Trade Secrets, 57 United States Attorneys' Bulletin, No. 5, 1-69 (Nov. 2009) (series of articles on prosecuting EEA cases), *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf; J. Michael Chamblee, *Validity, Construction, and Application of Title I of*

Economic Espionage Act of 1996 (18 U.S.C.A. §§ 1831 et seq.), 177 A.L.R. Fed. 609 (2002); James M. Fischer, Note, *An Analysis of the Economic Espionage Act of 1996*, 25 Seton Hall Legis. J. 239 (2001); Louis A. Karasik, *Under the Economic Espionage Act: Combating Economic Espionage is No Longer Limited to Civil Actions to Protect Trade Secrets*, 48 Fed. Law. 34 (2001); Michael Coblenz, *Intellectual Property Crimes*, 9 Alb. L.J. Sci. & Tech. 235 (1999); James H.A. Pooley, Mark A. Lemley & Peter J. Toren, *Understanding the Economic Espionage Act of 1996*, 5 Tex. Intell. Prop. L.J. 177 (1997).

B. The Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-1839

1. Overview

The Economic Espionage Act of 1996 ("EEA") promotes two primary and related objectives: to protect national and economic security. As noted in the House Report:

> With this legislation, Congress will extend vital federal protection to another form of proprietary economic information—trade secrets. There can be no question that the development of proprietary economic information is an integral part of America's economic well-being. Moreover, the nation's economic interests are a part of its national security interests. Thus, threats to the nation's economic interest are threats to the nation's vital security interests.

H.R. Rep. No. 104-788, at 4 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4023. President Clinton echoed these twin objectives in signing the legislation into law:

> Trade secrets are an integral part of virtually every sector of our economy and are essential to maintaining the health and competitiveness of critical industries operating in the United States. Economic espionage and trade secret theft threaten our Nation's national security and economic well-being.
>
> Until today, Federal law has not accorded appropriate or adequate protection to trade secrets, making it difficult to prosecute thefts involving this type of information. Law

> enforcement officials relied instead on antiquated laws that have not kept pace with the technological advances of modern society. This Act establishes a comprehensive and systemic approach to trade secret theft and economic espionage, facilitating investigations and prosecutions.

President William J. Clinton, Presidential Statement on the Signing of the Economic Espionage Act of 1996 (Oct. 11, 1996), *available at* 1996 Pub. Papers 1814 (Oct. 11, 1996).

The EEA criminalizes two types of trade secret misappropriation: economic espionage, under § 1831, and trade secret theft, under § 1832. In Title 18, § 1831 punishes the theft of a trade secret to benefit a foreign government, instrumentality, or agent:

> (a) In general.—Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—
>
> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
>
> (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
>
> (4) attempts to commit any offense described in any of paragraphs (1) through (3); or
>
> (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,
>
> shall, except as provided in subsection (b), be fined not more than $5,000,000 or imprisoned not more than 15 years, or both.

18 U.S.C. § 1831(a) (as amended by the Foreign and Economic Espionage Penalty Enhancement Act, Pub. L. No. 112-269, § 3, 126 Stat. 2442 (2013)) (emphasis added).

Section 1832, in contrast, punishes the commercial theft of trade secrets carried out for economic advantage, whether or not it benefits a foreign government, instrumentality, or agent:

> (a) Whoever, *with intent to convert a trade secret, that is related to a product or service used or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret,* knowingly—
>
> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
>
> (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
>
> (4) attempts to commit any offense described in paragraphs (1) through (3); or
>
> (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,
>
> shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

18 U.S.C. § 1832(a) (as amended by the Theft of Trade Secrets Clarification Act, Pub. L. No. 112-236, § 2, 126 Stat. 1627 (2012)) (emphasis added).

Although § 1831 (foreign economic espionage) and § 1832 (theft of trade secrets) define separate offenses, they are nevertheless related. The following

table highlights the common and distinct statutory language for both offenses, which are further discussed below:

	Section 1831(a) (Economic Espionage)	**Section 1832(a) (Theft of Trade Secrets)**
(1)	The defendant knowingly misappropriated information (e.g., possessed, stole, transmitted, downloaded) (or conspired or attempted to do so)	Same
(2)	The defendant knew or believed this information was proprietary and that he had no claim to it	Same
(3)	The information was in fact a trade secret (unless conspiracy or an attempt is charged)	Same
(4)	The defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality, or foreign agent	The defendant intended to convert the trade secret to the economic benefit of anyone other than the owner
(5)		The defendant knew or intended that the offense would injure the owner of the trade secret
(6)		The trade secret was related to a product or service used or intended for use in interstate or foreign commerce

Sections 1831(a) and 1832(a) both require the government to prove beyond a reasonable doubt that: (1) the defendant misappropriated information (or conspired or attempted to do so); (2) the defendant knew or believed this information was proprietary and that he had no claim to it; and (3) the information was in fact a trade secret (unless, as is discussed below, the crime charged is a conspiracy or an attempt). *See* 18 U.S.C. §§ 1831(a), 1832(a). Both sections criminalize trade secret misappropriations in a variety of forms, including but not limited to:

- stealing, taking or using fraud, artifice, or deception to obtain the trade secret, under §§ 1831(a)(1), 1832(a)(1);

- duplicating, taking photographs, downloading, uploading, altering, destroying, transmitting, or conveying the trade secret, under §§ 1831(a)(2), 1832(a)(2);
- receiving, buying or possessing the trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization, under §§ 1831(a)(3), 1832(a)(3).

To prove economic espionage under 18 U.S.C. § 1831, the government must also prove the defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality, or foreign agent.

If a foreign instrumentality element does not exist or cannot be proved, the government may still establish a violation of 18 U.S.C. § 1832 by proving, in addition to the first three elements described above, that: (4) the defendant intended to convert the trade secret to the economic benefit of anyone other than the owner; (5) the defendant knew or intended that the offense would injure the owner of the trade secret; and (6) the trade secret was related to a product or service used or intended for use in interstate or foreign commerce.

The EEA can be applied to a wide variety of criminal conduct. The statute criminalizes attempts and conspiracies to violate the EEA and certain extraterritorial conduct. See Sections B.6. and E.4. of this Chapter.

The EEA also provides several remedies that are unusual in a criminal statute: civil injunctive relief against violations, to be obtained by the Attorney General, 18 U.S.C. § 1836, and confidentiality orders to maintain the trade secret's secrecy throughout the prosecution, 18 U.S.C. § 1835. See Section D. of this Chapter. The statute includes an extraterritoriality provision, 18 U.S.C. § 1837, which extends its reach to conduct outside the United States where certain conditions are met. See Section E.4. of this Chapter.

For a discussion of the Department of Justice's oversight of and necessary approvals for EEA prosecutions, see Sections B.4, E.5.

2. Relevance of Civil Cases

The EEA's definition of a trade secret, 18 U.S.C. § 1839(3), is based in part on the trade secret definition in the Uniform Trade Secrets Act (UTSA), 14 U.L.A. 438 (1990). *See* H. R. Rep. No. 104-788, at 12 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4031. Cases that address trade secrets outside the EEA should, in most cases, be relevant in EEA prosecutions. *See generally United States v. Chung*, 659 F.3d 815 (9th Cir. 2011), *cert. denied*, _ U.S. _

(2012) (Because the EEA trade secret definition "is derived from the definition that appears in the Uniform Trade Secrets Act ... we consider instructive interpretations of state laws that adopted the UTSA definition without substantial modification") (footnote omitted); *Hsu*, 155 F.3d at 196 ("The EEA's definition of a 'trade secret' is similar to that found in a number of state civil statutes and the Uniform Trade Secrets Act ('UTSA'), a model ordinance which permits civil actions for the misappropriation of trade secrets. There are, though, several critical differences which serve to broaden the EEA's scope.") (footnote omitted).

3. Elements Common to 18 U.S.C. §§ 1831, 1832

As discussed below, a trade secret consists of three primary components: (1) information; (2) which derives independent economic value from being secret; and (3) that the owner took reasonable measures to protect. *See also ConFold Pac., Inc. v. Polaris Indus.*, 433 F.3d 952, 959 (7th Cir. 2006) (Posner, J.) (noting a trade secret can be any information, whether in tangible form or otherwise, that its owner takes reasonable measures to keep secret, and that has some economic value as a result of its secrecy) (citations omitted).

The elements for completed offenses are discussed in the ensuing sections. Attempts and conspiracies are discussed in Section B.6. of this Chapter.

a. The Information Was a Trade Secret

The government should ascertain the specific information the victim claims is a trade secret at the outset of the investigation. "[A] prosecution under [the EEA] must establish a particular piece of information that a person has stolen or misappropriated." 142 Cong. Rec. 27, 117 (1996). This will help avoid the defendant's defense that he was merely relying on his general knowledge, skills, and abilities along, perhaps, with legitimate reverse engineering. See Section C.3. of this Chapter. Other questions to consider include how many trade secrets may have been misappropriated and how they relate to one another.

In ascertaining what is the trade secret and the number of trade secrets in a particular case, consider who would be the best trial witness to testify about these issues before the jury. For example, where source code is the trade secret, the chief technology officer, or other supervisor overseeing the project development, may be an appropriate witness. In other cases, a chief engineer may be a suitable witness, depending on the nature of the trade secret.

The defense, however, has no right to take pre-trial depositions of the government's expert witnesses to determine what the government will claim is a trade secret and why. *See United States v. Ye*, 436 F.3d 1117, 1123 (9th Cir. 2006) (granting government's petition for a writ of mandamus and rescinding trial court order for deposition of the government's expert witnesses).

i. "Information"

Whether particular information is a trade secret is a question of fact. *See, e.g.*, *Hoechst Diafoil Co. v. Nan Ya Plastics Corp.*, 174 F.3d 411, 419 (4th Cir. 1999) (noting that whether or not a trade secret exists is a "fact-intensive question to be resolved upon trial"); *see also* 4 Roger M. Milgrim, *Milgrim on Trade Secrets* § 15.01[1][a][i].

The EEA defines a trade secret very broadly to include all types of information, regardless of the method of storage or maintenance, that the owner has taken reasonable measures to keep secret and that itself has independent economic value. Specifically, §1839(3) states:

> (3) the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if —
>
> > (A) the owner thereof has taken reasonable measures to keep such information secret; and
> >
> > (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

18 U.S.C. § 1839(3). The statute's legislative history also counsels a broad interpretation of this definition. *See* H.R. Rep. No. 104-788, at 12 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4031. In addition, because the EEA's definition of a trade secret derives in part from civil law, civil cases that address trade secrets outside the EEA should, in most cases, be helpful in EEA prosecutions. See Section B.2. of this Chapter.

Examples of trade secrets in criminal prosecutions include:

- Processes, methods, and formulas for an anti-cancer drug known as Taxol. *United States v. Hsu*, 155 F.3d 189 (3rd Cir. 1998)
- Cost information unavailable to the public, confidential business plan, and customer list. *United States v. Martin*, 228 F.3d 1 (1st Cir. 2000)
- Measurements, metallurgical specifications, and engineering drawings to produce an aircraft brake assembly. *United States v. Lange*, 312 F.3d 263 (7th Cir. 2002)
- Adhesive product information. *United States v. Yang*, 281 F.3d 534 (6th Cir. 2002)
- Microsoft windows source code. *United States v. Genovese*, 409 F. Supp. 2d 253 (S.D.N.Y. 2005)
- Coca–Cola documents and product samples. *United States v. Williams*, 526 F.3d 1312 (11th Cir. 2008) (*per curiam*)
- Biological strains and plasmids. *United States v. Huang*, Nos. 1:10-cr-102, 1:11-cr-163 (S.D. Ind. 2010)
- Documents relating to the Space Shuttle, Delta IV and C-17. *United States v. Chung*, 633 F. Supp. 2d 1134 (C.D. Cal. 2009), *aff'd*, 659 F.3d 815 (9th Cir. 2011), *cert. denied*, _ U.S. _ (2012)
- Photographs of tire-assembly machine. *United States v. Howley*, __F.3d__, 2013 WL 399345, at *3 (6th Cir. Feb. 4, 2013).

For an extensive collection of cases analyzing whether specific types of information constitute a trade secret, see 1 *Milgrim on Trade Secrets* § 1.09. In cases alleging attempt and conspiracy, the government need not prove that the information actually was a trade secret. See Section B.6. of this Chapter.

ii. Secrecy

The key attribute of a trade secret is that the underlying information "not be[] generally known to ... the public" and that it "not be[] readily ascertainable through proper means by [] the public." 18 U.S.C. § 1839(3)(B).

Unlike other forms of intellectual property, a trade secret need only possess "minimal novelty." *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974) (quoting Comment, *The Stiffel Doctrine and the Law of Trade Secrets*, 62 Nw. U. L. Rev. 956, 969 (1968)); *see also Avidair Helicopter Supply, Inc. v. Rolls-Royce Corp.*, 663 F.3d 966, 972 (8th Cir. 2011) (finding "existence of a trade secret is determined by the value of a secret, not the merit of its technical improvements"); *Learning Curve Toys, Inc. v. Playwood Toys, Inc.*, 342 F.3d 714,

724 (7th Cir. 2003) (finding that, in contrast to "a patentable invention, a trade secret need not be novel or unobvious."); *Avtec Sys., Inc. v. Peiffer*, 21 F.3d 568, 575 (4th Cir. 1994) (holding that the "hallmark of a trade secret is not its novelty but its secrecy"); *Arco Indus. Corp. v. Chemcast Corp.*, 633 F.2d 435, 442 (6th Cir. 1980) (trade secret need only minimal novelty). This has been defined as some element that sets the information apart from what is generally known. "While we do not strictly impose a novelty or inventiveness requirement in order for material to be considered a trade secret, looking at the novelty or uniqueness of a piece of information or knowledge should inform courts in determining whether something is a matter of general knowledge, skill or experience." 142 Cong. Rec. 27, 117 (1996); *see also Hertz v. Luzenac Grp.*, 576 F.3d 1103, 1110 (10th Cir. 2009) (observing that "[a] finding that some of the elements are secret may support a conclusion that the entire process is protected"); c*f. Buffets, Inc. v. Klinke*, 73 F.3d 965, 968 (9th Cir. 1996) (holding that plaintiff's recipes were not trade secrets in part because they lacked the requisite novelty).

Whether the term "public" in 18 U.S.C. § 1839(3)(B) refers to the general public or those with general skills in a particular trade or industry has been the subject of litigation. "[E]ither the phrase 'readily ascertainable' or the phrase 'the public' must be understood to concentrate attention on either potential users of the information, or proxies for them (which is to say, persons who have the same ability to 'ascertain' the information)." *United States v. Lange*, 312 F.3d 263, 268 (7th Cir. 2002) (Easterbrook, J.). *But see id.* at 271-72 (Ripple, J., concurring) (suggesting that this holding is dictum); *see also Chung*, 659 F.3d at 825 (noting open issue and "some conflict between circuits" on this issue). In other words, information will not necessarily be a trade secret just because it is not readily ascertainable by the general public. Under the Seventh Circuit's view, the information may not be a trade secret if it is readily ascertainable by those within the information's field of specialty.

If a scientist could ascertain a purported trade secret formula only by gleaning information from publications and then engaging in many hours of laboratory testing and analysis, the existence of such publications would not necessarily disqualify the formula as a trade secret under the EEA, since the scientist's work may probably not qualify as "readily ascertainable through proper means by, the public." *See* 18 U.S.C. § 1839(3)(B). But the formula would not be a trade secret if it could be ascertained or reverse engineered within a relatively short time or through the expenditure of few resources.

See Lange, 312 F.3d at 269 (EEA case) ("Such measurements could not be called trade secrets if ... the assemblies in question were easy to take apart and measure."); *Buffets, Inc. v. Klinke*, 73 F.3d 965, 968 (9th Cir. 1996) (holding restaurant chain's recipes were not trade secrets because, although innovative, the recipes were readily ascertainable by others); *Marshall v. Gipson Steel, Inc.*, 806 So.2d 266, 271-72 (Miss. 2002) (holding that company's bid estimating system was readily ascertainable by using simple math applied to data on past bids, and thus was not a trade secret); *Weins v. Sporleder*, 569 N.W.2d 16, 20-21 (S.D. 1997) (holding formula of cattle feed product was not a trade secret because the ingredients could be determined through chemical or microscopic analysis in four or five days, at most, and for about $27).

iii. Elements in the Public Domain

A trade secret can include elements that are in the public domain if the trade secret itself constitutes a unique, "effective, successful and valuable integration of the public domain elements." *Rivendell Forest Prods., Ltd. v. Georgia-Pacific Corp.*, 28 F.3d 1042, 1046 (10th Cir. 1994); *accord Tewari De-Ox Sys., Inc. v. Mountain States/Rosen, L.L.C.*, 637 F.3d 604, 613 (5th Cir. 2011); *Strategic Directions Grp., Inc. v. Bristol-Myers Squibb Co.*, 293 F.3d 1062, 1065 (8th Cir. 2002); *Metallurgical Indus., Inc. v. Fourtek, Inc.*, 790 F.2d 1195, 1202 (5th Cir. 1986); *Servo Corp. of America v. General Electric Co.,* 393 F.2d 551, 554 (4th Cir.1968) (holding that a trade secret "might consist of several discrete elements, any one of which could have been discovered by study of material available to the public"); *Apollo Techs. Corp. v. Centrosphere Indus.*, 805 F. Supp. 1157, 1197 (D.N.J. 1992). In fact, "[a] trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain, but the unified process, design and operation of which, in unique combination, affords a competitive advantage and is a protectable secret." *Metallurgical Indus.*, 790 F.2d at 1202 (quoting *Imperial Chem., Ltd. v. National Distillers & Chem. Corp.*, 342 F.2d 737, 742 (2d Cir. 1965)); *accord Hertz v. Luzenac Grp.*, 576 F.3d 1103, 1109-10 (10th Cir. 2009); *Mike's Train House, Inc. v. Lionel, L.L.C.*, 472 F.3d 398, 411 (6th Cir. 2006); *Harvey Barnett, Inc. v. Shidler*, 338 F.3d 1125,1130 (10th Cir. 2003); *3M v. Pribyl*, 259 F.3d 587, 595-96 (7th Cir. 2001); *Integrated Cash Mgmt. Servs., Inc. v. Digital Transactions, Inc.*, 920 F.2d 171, 174 (2d Cir. 1990); *Syntex Ophthalmics, Inc. v. Tsuetaki*, 701 F.2d 677, 684 (7th Cir. 1983); *Rivendell Forest Prods.*, 28 F.3d at 1046. For example, in *Metallurgical Industries*, when the company modified a generally-known zinc recovery process, the modified

process could be considered a trade secret even though the original process and the technologies involved were publicly known, because the details of the modifications were not. 790 F.2d at 1201-03.

The definition of a trade secret under 18 U.S.C. § 1839(3) includes "compilations." The courts have consistently recognized that a compilation which includes publicly known elements may still qualify as a trade secret so long as the unified information satisfies the requirements to establish a trade secret. *See, e.g., AvidAir Helicopter Supply, Inc. v. Rolls-Royce Corp.*, 663 F.3d 966, 972 (8th Cir. 2011) ("Compilations of non-secret and secret information can be valuable so long as the combination affords a competitive advantage and is not readily ascertainable."); *Decision Insights, Inc. v. Sentia Group, Inc.*, 311 Fed. Appx. 586, at 592-94 (4th Cir. 2009) (per curiam) (noting that a software compilation can qualify for protection as a trade secret); *3M v. Pribyl*, 259 F.3d 587, 586 (7th Cir. 2001) (trade secret established for operating procedures and manuals which included material in the public domain, concluding that "when all the cleaning procedures, temperature settings, safety protocols, and equipment calibrations are collected and set out as a unified process, that compilation, if it meets the other qualifications, may be considered a trade secret"); *Imperial Chem. Indus. v. Nat'l Distillers and Chem. Corp.*, 342 F.2d 737, 740 (2d Cir. 1965) (while eight of the nine components for a chemical process were in the public domain, the "unified description of the design, process and operation, i.e, the way in which the features were interrelated" constituted a trade secret); *see also Penalty Kick Mgmt. Ltd. v. Coca Cola Co.*, 318 F.3d 1284, 1291 (11th Cir. 2003) ("even if all of the information is publicly available, a unique combination of that information, which adds value to the information, also may qualify as a trade secret").

iv. Independent Economic Value

The trade secret must derive "independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by, the public." 18 U.S.C. § 1839(3)(B). Although the EEA does not require the government to prove a specific level of value, the government must prove that the secret has some value. Economic value "speaks to the value of the information to either the owner or a competitor; any information which protects the owner's competitive edge or advantage." *US West Communications, Inc. v. Office of Consumer Advocate*, 498 N.W.2d 711, 714 (Iowa 1993) (citations omitted). "[I]nformation kept secret that would be useful to a competitor and require cost, time and effort to duplicate is of economic value." *Id.* (citation

omitted); *see also Trandes Corp. v. Guy F. Atkinson Co.*, 996 F.2d 655, 663 (4th Cir. 1993) (object code derived independent economic value from secrecy where the trade secret owner "generates most of its revenues by providing computer services to engineering firms and construction companies" and "receives raw data from its clients, processes the data with the Tunnel System software, and reports the results back to the clients"; "[a]rmed with a copy of the object code, an individual would have the means to offer much the same engineering services as" the trade secret owner). Independent economic value can be shown even where there are no direct competitors for the particular trade secret but disclosure would confer advantages to competitors. *See, e.g.*, *Chung*, 659 F.3d at 827 ("Although Boeing had no competitors for the integration project itself, ... [a] reasonable inference is that the information could assist a competitor in understanding how Boeing approaches problem-solving and in figuring out how best to bid on a similar project in the future, for example, by underbidding Boeing on tasks at which Boeing appears least efficient.").

The secret's economic value can be demonstrated by the circumstances of the offense, such as the defendant's acknowledgment that the secret is valuable, the defendant's asking price, or an amount of time or money the defendant's buyers would have required to replicate the information. *See United States v. Lange*, 312 F.3d 263, 269 (7th Cir. 2002); *United States v. Genovese*, 409 F. Supp. 2d 253, 257 (S.D.N.Y. 2005).

Not all of a business's confidential information may be valuable in a competitor's hands. For example, in *Microstrategy, Inc. v. Business Objects, S.A.*, 331 F. Supp. 2d 396, 421 (E.D. Va. 2004), the court found that a company-wide email concerning the firm's financial problems and plans for survival was not a trade secret because it was unclear what economic value it would have had to anyone outside the company. *See also US West Communications*, 498 N.W.2d at 715 (finding no evidence of economic value without evidence that disclosure would have harmed the victim).

Customer Lists or Information

Some information that a company deems proprietary may not qualify as a trade secret. For example, under the Uniform Trade Secrets Act—which defines trade secrets in a manner similar to the EEA—a customer list is generally a trade secret only if the customers are not known to others in the industry, could be discovered only by extraordinary efforts, and the list was developed through a substantial expenditure of time and money. *See ATC Distribution Group v.*

Whatever It Takes Transmissions & Parts, 402 F.3d 700, 714-15 (6th Cir. 2005); *Conseco Fin. Servicing Corp. v. North Am. Mortgage Co.*, 381 F.3d 811, 819 & n.6 (8th Cir. 2004) (holding files of thousands of customers nationwide who were identified through a complex computer system to be trade secrets); *United States v. Martin*, 228 F.3d 1, 12 n.8 (1st Cir. 2000) (noting customer list could qualify as a trade secret); *A.F.A. Tours, Inc. v. Whitchurch*, 937 F.2d 82, 89 (2d Cir. 1991) (customer list from tour agency could qualify as a trade secret); *Surgidev Corp. v. Eye Technology, Inc.*, 828 F.2d 452, 455 & n.3 (8th Cir. 1987) (ophthalmologist customer information on high volume implanters of surgically implanted intraocular lenses devices qualified as a trade secret); *Leo Silfen, Inc. v. Cream*, 278 N.E.2d 636, 639-41 (N.Y. 1972). Some state statutes, based on Section 1(4) of the Uniform Trade Secret Act, expressly include customer lists within the definition of a trade secret.

Whether a customer list qualifies as a trade secret depends on the facts. For example, a customer list is less likely to be considered a trade secret if customers' identities are readily ascertainable to those outside the list-owner's business and the list was compiled merely through general marketing efforts. *See ATC Distribution Group*, 402 F.3d at 714-15 (affirming that customer list of transmission parts customers was not a trade secret because names of purchasers could "be ascertained simply by calling each shop and asking"); *Nalco Chem. Co. v. Hydro Techs., Inc.*, 984 F.2d 801, 804 (7th Cir. 1993) (holding that customer list was not a trade secret when base of potential customers was "neither fixed nor small"); *Standard Register Co. v. Cleaver*, 30 F. Supp. 2d 1084, 1095 (N.D. Ind. 1998) (holding that customer list was not a trade secret where owner's competitors knew customer base, knew other competitors quoting the work, and were generally familiar with the customers' needs).

v. Reasonable Measures

Trade secrets are fundamentally different from other forms of property in that a trade secret's owner must take reasonable measures under the circumstances to keep the information confidential. *See* 18 U.S.C. § 1839(3)(A); *Lange*, 312 F.3d at 266. This requirement is generally not imposed upon those who own other types of property. For example, a thief can be convicted for stealing a bicycle the victim left unlocked in a public park, whereas a thief might not be convicted under the EEA for stealing the bicycle's design plans if the victim left the plans in a public park.

For these reasons, prosecutors and investigators should identify the measures the victim used to protect the trade secret early in their investigation. These protections will be a critical component of the case or the decision not to prosecute. One means of identifying the reasonable measures safeguarding the trade secret is to visit the facility. The barriers to access may be more readily apparent by viewing the circumstances and surroundings.

Whether reasonable efforts have been employed is normally a question of fact for the fact-finder. *See, e.g.*, *Camp Creek Hospitality Inns, Inc. v. Sheraton Franchise Corp.*, 139 F.3d 1396, 1411 (11th Cir. 1998) ("Whether Camp Creek's efforts to keep the information secret in this case were 'reasonable under the circumstances' presents a question for the trier of fact."); *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 197 (7th Cir. 1991) ("But only in an extreme case can what is a 'reasonable' precaution be determined on a motion for summary judgment, because the answer depends on a balancing of costs and benefits that will vary from case to case and so require estimation and measurement by persons knowledgeable in the particular field of endeavor involved.").

Depending on the trade secret being protected, security measures may include physical safeguards, network security, and contractual protections. These measures may include:

Physical Security

- Restricting employee access to building areas, based on a need to know;
- Requiring identification and access badges intended to limit access to restricted areas;
- Keeping the secret physically secure in locked drawers, cabinets, or rooms;
- Restricting visitors from accessing areas where confidential information is kept;
- Requiring visitors to obtain clearance prior to visit, pass through security checkpoints and be escorted by an employee at all times; and,
- Securing buildings with fences, locked doors and guards.

Network Security

- Encrypting sensitive electronic information, such as uncompiled source code;

- Protecting computer files and directories with passwords and recurring password changes;
- Employing corporate firewalls and virtual private networks for remote access;
- Restricting employees from using unapproved peripherals, such as high capacity portable storage devices; and
- Maintaining of network logs.

Contractual and Employment Practices

- Restricting access to those with a need to know;
- Splitting tasks among people or teams to avoid concentrating too much information in any one place;
- Requiring recipients, including employees, contractors and business partners, to sign confidentiality, non-disclosure, or non-competition agreements;
- Marking documents as confidential, proprietary, or secret;\
- Providing regular training concerning steps to safeguard trade secrets; and
- Conducting exit interview once employee leaves company, and confirming confidentiality obligations with departing employee.

See also Chung, 659 F.3d at 825 ("Security measures, such as locked rooms, security guards, and document destruction methods, in addition to confidentiality procedures, such as confidentiality agreements and document labeling, are often considered reasonable measures."); *Lange*, 312 F.3d at 266 (EEa case concerning aircraft brake assemblies); *Reingold v. Swiftships, Inc.*, 126 F.3d 645, 650 (5th Cir. 1997) (discussing steps to protect ship-builder's mold for fiberglass boat hulls); 1 Roger M. Milgrim, *Milgrim on Trade Secrets* § 1.04.

The owner's security measures need not be absolute or the best available, and need only satisfy the standard of reasonableness under the facts and circumstances of the specific case. *See* H.R. Rep. No. 104-788, at 7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4026 ("[A]n owner of this type of information need only take 'reasonable' measures to protect this information…. [I]t is not the Committee's intent that the owner be required to have taken every conceivable step to protect the property from misappropriation."); *Howley,* 2013 WL 399345, at *3 ("[t]he 'reasonable measures' requirement does not mean a company must keep its own employees and suppliers in the dark about machines they need to do their work"); *Lange*, 312 F.3d at 266; *Surgidev Corp. v. Eye Tech., Inc.*, 828 F.2d 452, 455 (8th Cir. 1987) ("Only reasonable efforts,

not all conceivable efforts, are required to protect the confidentiality of putative trade secrets."); *see also Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc.*, 35 F.3d 1226, 1235-36 (8th Cir. 1994) (discussing steps to safeguard genetic messages of genetically engineered corn); *Gates Rubber Co. v. Bando Chem. Indus.*, 9 F.3d 823, 848-49 (10th Cir. 1993) (discussing steps to protect industrial belt replacement software); *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 521 (9th Cir. 1993) (noting reasonable measures such as requiring "employees to sign confidentiality agreements respecting [company's] trade secrets"); *K-2 Ski Co. v. Head Ski Co.,* 506 F.2d 471, 473-74 (9th Cir. 1974) (discussing steps to protect design and manufacture specifications of high performance skis); *Elm City Cheese Co. v. Federico*, 752 A.2d 1037, 1049-53 (Conn. 1999) (holding that victim's failure to require defendant employee to sign a confidentiality, non-disclosure, or non-competition agreement was reasonable "in light of the close personal relationship enjoyed over the years" by the parties); 1 *Milgrim on Trade Secrets* § 1.04.

A recent Ninth Circuit decision, *United States v. Chung*, underscores the requirement that only reasonable measures are necessary to satisfy this element. In considering a sufficiency of the evidence claim, the court considered whether reasonable measures were employed to safeguard a trade secret (phased array antenna documents for the space shuttle) which was not secured by locks. Taken as a whole, other measures were reasonable. As the court noted:

> Although none of the documents was kept under lock and key, Boeing implemented general physical security measures for its entire plant. Security guards required employees to show identification before entering the building, and Boeing reserved the right to search all employees' belongings and cars. Boeing also held training sessions instructing employees not to share documents with outside parties, and it required employees, including Defendant, to sign confidentiality agreements. Further, two of the four phased array documents (underlying counts 3 and 5) were marked as proprietary. Thus, there was sufficient evidence to support the conclusion that Boeing took reasonable measures to keep all four phased array antenna documents secret.

Chung, 659 F.3d at 827.

It is important that the reasonable measures standard is appropriately and fairly applied. Courts have held that the focus of reasonableness should be on the measures that were taken, not on other measures that could have been taken, particularly with the benefit of hindsight. For example, the Tenth Circuit reversed a summary judgment based on misapplication of the reasonableness standard. Specifically, the trial court erred "in considering whether Luzenac adequately protected the secrecy of [trade secret] 604AV, the district court focused on the evidence of the steps that Luzenac did not take rather than the reasonableness of the measures it did take." *Hertz v. Luzenac Group*, 576 F.3d 1103, 1109 (10th Cir. 2009). The court observed: "[T]here always are more security precautions that can be taken. Just because there is something else that Luzenac could have done does not mean that their efforts were unreasonable under the circumstances." *Id*. at 1113; *see also General Universal Sys., Inc. v. Lee*, 379 F.3d 131, 150 (5th Cir. 2004) (concluding the district erroneously "focused solely on Lopez's alleged failure to take 'reasonable precautions' to protect" the trade secret where there was "uncontroverted evidence that" reasonable precautions were taken). Additionally, courts have held that "the fact that one 'could' have obtained a trade secret lawfully is not a defense if one does not actually use proper means to acquire the information." *Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc.*, 35 F.3d 1226, 1237 (4th Cir. 1994) (citations omitted); *see also Wyeth v. Natural Biologics, Inc.*, 395 F.3d 897, 899-900 (8th Cir. 2005) (rejecting claim that the trade secret owner "failed to adequately secure its trade secret in many [specified] ways" and concluding sufficient reasonable measures included "use of physical security, limited access to confidential information, employee training, document control, and oral and written understandings of confidentiality").

If a trade secret was disclosed to licensees, vendors, or third parties for limited purposes, those disclosures do not waive trade secret protections so long as the trade secret owner took reasonable security measures before and during disclosure, such as requiring non-disclosure agreements from all recipients. *See, e.g.*, *Howley*, 2013 WL 399345, at *4; *Quality Measurement Co. v. IPSOS S.A.,* 56 Fed. Appx. 639, 647 (6th Cir. 2003); *MAI Sys. Corp.*, 991 F.2d at 521; *Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs.*, 923 F. Supp. 1231, 1254 (N.D. Cal. 1995). However, other reasonable measures may be adopted instead. For example, where the trade secret owner "relies on *deeds* (the splitting of tasks) rather than *promises* to maintain confidentiality," it is "irrelevant that [the victim] does not require vendors to sign confidentiality agreements." *Lange,* 312 F.3d at 266 (emphasis in original).

As discussed above, information does not lose its status as a trade secret if it is disclosed to the government for purposes of investigation or prosecution. For this reason, federal prosecutors and law enforcement agents need not sign protective orders with victims before accepting trade secret information.

A defendant who was unaware of the victim's security measures can be convicted under the EEA if he was aware that the misappropriated information was proprietary. *United States v. Krumrei*, 258 F.3d 535, 538-39 (6th Cir. 2001) (rejecting void-for-vagueness argument against EEA); *accord United States v. Genovese*, 409 F. Supp. 2d 253, 258 (S.D.N.Y 2005) ("In this case, one can infer that Genovese knew not only that the source code was proprietary, but that any protective measures by Microsoft had been circumvented."). There is no requirement that a defendant be aware that the victim implemented security measures to protect the misappropriated information.

b. Misappropriation

i. Means of Misappropriation

Under § 1831 and § 1832, a defendant must have misappropriated the trade secret through one of the acts prohibited in §§ 1831(a)(1)-(5) or 1832(a)(1)-(5), respectively. Misappropriation covers a broad range of acts including traditional methods of theft in which a trade secret is physically removed from the owner's possession, and also less traditional methods of misappropriation such as copying, duplicating, sketching, drawing, photographing, downloading, uploading, altering, destroying, photocopying, replicating, transmitting, delivering, sending, mailing, communicating, or conveying the information. *See* 18 U.S.C. §§ 1831(a)(1)-(2), 1832(a)(1)-(2). Although many of these means of misappropriation leave the original property in the hands of its owner, they reduce or destroy the trade secret's value nonetheless. Congress prohibited all types of misappropriation "to ensure that the theft of intangible information is prohibited in the same way that the theft of physical items is punished." H.R. Rep. No. 104-788, at 11 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4030. Misappropriation also includes the knowing receipt, purchase, or possession of trade secrets. *See* 18 U.S.C. §§ 1831(3), 1832(3).

Because §§ 1831 and 1832 do not contain a specific statute of limitations, the general five-year statute of limitations for non-capital offenses applies. *See* 18 U.S.C. § 3282. In one recent prosecution for economic espionage (*United States v. Chung*), however, the court held misappropriation that occurred before the five-year statute of limitation does not defeat a trade secret prosecution

because possession of trade secrets is a "continuing offense." In *Chung*, the defendant, a former Boeing employee, misappropriated trade secrets before the five-year statute of limitations period (2003 through 2008) and included conduct that occurred during the late 1970s. The court concluded that trade secrets misappropriated before the period of the statute of limitations, yet possessed within the period of the statute of limitations may violate the statute so long as the remaining elements of the offense are satisfied. *See Chung*, 633 F. Supp. 2d at 1146 n.12 ("Because Mr. Chung continued to possess the documents in 2006, there is no statute of limitations problem here. [P]ossessory offenses have long been described as 'continuing offenses' that are not complete upon receipt of the prohibited item. Rather, the statute of limitations does not begin to run until the possessor parts with the item.") (quotation marks and citation omitted). On appeal, the Ninth Circuit affirmed, concluding that the conspiracy to violate the EEA was established by proof that the agreement between the defendant and his co-conspirators "continued into the limitations period." *Chung*, 659 F.3d at 828; *see also id.* ("Given Defendant's history of passing technical documents to China, however, a rational trier of fact reasonably could infer from Defendant's more recent possession of similar documents that his intent to benefit China persisted well into the limitations period and extended to his possession of the trade secrets.").

When charging trade secret theft or economic espionage under 18 U.S.C. §§ 1831 and 1832 the prosecutor may charge each means of theft as a separate count. For example, where the defendant takes a trade secret prototype from his employer's facility, and also emails trade secret design schematics to a competitor, the prosecutor may include a count for violation of § 1832(a)(1) with respect to the stealing of the prototype and a separate count for violation of § 1832(a)(2) with respect to the emailing of the design specifications. A prosecutor may also wish to consider what other legal theories may apply to the facts of the case. See Section G. of this chapter for other charges to consider.

ii. Memorization Included

The above types of misappropriation include not only manipulating a physical object, but also conveying or using intangible information that has been memorized. The EEA defines a trade secret as "*all forms and types* of financial, business, scientific, technical, economic, or engineering *information*, ... *whether tangible or intangible*, and whether or how stored." 18 U.S.C. § 1839(3) (emphasis added). The statute also prohibits not only actions taken against a trade secret's physical form, such as "steal[ing], ...tak[ing], [and]

carr[ying] away", 18 U.S.C. §§ 1831(a)(1), 1832(a)(1), but also actions that can be taken against a trade secret in a memorized, intangible form, such as "sketch[ing], draw[ing], ... download[ing], upload[ing], ..., transmit[ting], ... communicat[ing], [and] convey[ing]," 18 U.S.C. §§ 1831(a)(2), 1832(a)(2). *See* James H.A. Pooley et al., *Understanding the Economic Espionage Act of 1996*, 5 Tex. Intell. Prop. L.J. 177 (1997). In this respect, as in others, the EEA echoes civil law and some pre-EEA caselaw. *See, e.g.*, *Stampede Tool Warehouse, Inc. v. May*, 651 N.E.2d 209, 217 (Ill. App. Ct. 1995) ("A trade secret can be misappropriated by physical copying or by memorization.") (citations omitted); 4 Roger M. Milgrim, *Milgrim on Trade Secrets* § 15.01[e]. Trade secret cases to the contrary that do not involve the EEA are not persuasive authority on this point.

This is not to say, however, that any piece of business information that can be memorized is a trade secret. As noted, the EEA does not apply to individuals who seek to capitalize on their lawfully developed knowledge, skill, or abilities. When the actions of a former employee are unclear and evidence of theft has not been discovered, it may be advisable for a company to pursue its civil remedies and make another criminal referral if additional evidence of theft is developed.

Where available, tangible evidence of theft or copying is helpful in all cases to overcome the potential problem of prosecuting the defendant's purported "mental recollections" and a defense that "great minds think alike."

iii. Lack of Authorization

The crux of misappropriation is that the defendant acted "without authorization" from the trade secret's owner. The necessary "authorization is the permission, approval, consent or sanction of the owner" to obtain, destroy, or convey the trade secret. 142 Cong. Rec. 27,116 (1996). Thus, although an employee may be authorized to possess a trade secret during his employment, he would violate the EEA if he conveyed it to a competitor without his employer's permission.

iv. Misappropriation of Only Part of a Trade Secret

A defendant can be prosecuted even if he misappropriated only part of a trade secret. Using only part of the secret, so long as it too is secret, qualifies as misappropriation. *Mangren Research and Dev. Corp. v. National Chem. Co.*, 87 F.3d 937, 943-44 (7th Cir. 1996); *cf. United States v. Pemberton*, 904 F.2d 515,

517 (9th Cir. 1990) (rejecting argument of defendant convicted for receiving 30 stolen technical landscape and irrigation drawings for a commercial development "that the incomplete nature of the drawings rendered them worthless," because evidence established that "some of the drawings would have been useful to the developer, even though not entirely finished," and the developer might have been willing to adjust the price for the drawings' incomplete nature); *United States v. Inigo*, 925 F.2d 641, 653-54 (3d Cir. 1991) (Hobbs Act conviction) (rejecting defendant's argument that the victim should not have feared economic loss because, *inter alia*, he possessed less than five percent of the confidential documents on a subject, and holding that "what matters is how important the documents [the defendant] had were to [the defendant], not their number").

v. Mere Risk of Misappropriation Not Prosecutable, but Attempts and Conspiracies Are

A former employee cannot be prosecuted just because she was exposed to a trade secret at her former job and has now moved to a competitor. The government must establish that she knowingly stole or misappropriated a particular trade secret and did so with the "intent to convert a trade secret ... to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret." 18 U.S.C. § 1832(a). The intent element is considered further below.

c. Knowledge

The EEA contains a heightened *mens rea* requirement. Section 1831 requires that the government prove that the defendant (1) knowingly misappropriated a trade secret (e.g., possessed, stole, transmitted, downloaded) and (2) did so with the intent, "or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent." Section 1832 requires that the government show that the defendant (1) knowingly misappropriated a trade secret (e.g., possessed, stole, transmitted, downloaded) and (2) did so "with intent to convert a trade secret ... to the economic benefit of anyone other than the owner" and (3) "intending or knowing that the offense will, injure any owner of that trade secret."

As outlined above, the first part of the *mens rea* requirement in an EEA case is that the defendant misappropriated the trade secret "knowingly." As noted in the legislative history, "A knowing state of mind with respect to an element of the offense is (1) an awareness of the nature of one's conduct, and

(2) an awareness of or a firm belief in or knowledge to a substantial certainty of the existence of a relevant circumstance, such as whether the information is proprietary economic information as defined by this statute." S. Rep. No. 104-359, at 16 (1996).

Based upon the legislative history, the government is not required to prove that the defendant knew and understood the statutory definition of a trade secret, as set forth in 18 U.S.C. § 1839(3), before acting. If the government had to prove this, the EEA would be unnecessarily narrowed in its application, which is contrary to the intent of Congress. Some violations would be nearly impossible to prosecute in a number of factual scenarios, and would amount to a willfulness *mens rea* requirement equivalent to that imposed for criminal copyright infringement. For example, as part of protecting and limiting a trade secret to those on a need to know basis, some companies do not divulge all of the reasonable measures used to protect the trade secret, even within the company. The individual stealing a trade secret may not know about these reasonable measures safeguarding the trade secret.

The legislative history is clear that Congress intended to extend the reach of the new federal offenses involving trade secret misappropriation. In fact, the legislative history supports a "knew or should have known" *mens rea* requirement:

> It is not necessary that the government prove that the defendant knew his or her actions were illegal, rather the government must prove that the defendant's actions were not authorized by the nature of his or her relationship to the owner of the property and that the defendant *knew or should have known* that fact.

H.R. Rep. No. 104-788, at 12 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4030-31 (emphasis added); 142 Cong. Rec. 27,117 (1996) (government must show the defendant was "aware or substantially certain" he was misappropriating a trade secret); *see also United States v. Genovese*, 409 F. Supp. 2d 253, 258 (S.D.N.Y. 2005) (discussing circumstances that would indicate that EEA defendant knew the information was proprietary).

Congress did not require the government to show that the defendant specifically was aware of each element of the definition of a trade secret under § 1839(3) (e.g., that the defendant knew of specific reasonable measures employed by the trade secret owner to protect the trade secret). An opportunistic defendant, such as a company outsider, may not be fully

aware of all of the company measures used to safeguard a trade secret, but does know the proprietary information has value which he intends to use to injure the owner of the trade secret. In other words, the defendant knowingly misappropriated property (or proprietary information) belonging to someone else without permission. In fact, in recognizing this point, the Sixth Circuit has held that the "defendant need not have been aware of the particular security measures taken by [the trade secret owner]. Regardless of his knowledge of those specific measures, defendant knew the information was proprietary." *Krumrei*, 258 F.3d at 539 (affirming denial of motion to dismiss indictment as void for vagueness); *see also United States v. Roberts*, No. 3:08-CR-175, 2009 WL 5449224, at *7 (E.D. Tenn. Nov. 17, 2009) (holding that "a defendant must know that the information he or she seeks to steal is proprietary, meaning belonging to someone else who has an exclusive right to it, but does not have to know that it meets the statutory definition of a trade secret"), *report and recommendation adopted by*, 2010 WL 56085 (E.D. Tenn. Jan. 5, 2010) (quoting H.R. Rep. No. 104-788, at 12 (1996)).

An example demonstrates why it logically follows that the government is not required to prove the defendant was aware of each of the sub-elements of the trade secret definition under §1839(3), including his knowledge of the trade secret owner's specific reasonable measures taken to safeguard the trade secret. Assume a hacker infiltrates a company's corporate network and copies sensitive research and development materials regarding a product the company is developing for future release. The hacker may not know all the steps the company has taken to protect its information such as requiring its employees to sign non-disclosure agreements, employing physical security measures at its offices or restricting sensitive information to its employees on a need-to-know basis. However, the hacker did overcome the company's electronic security measures and knowingly misappropriated sensitive research and development information, which he shared with others, either intending to benefit another country or injure the owner of the trade secret. By the nature of his relationship with the trade secret owner, the defendant is aware the property belongs to someone else and that he misappropriated it without the authorization of the company**.**

As already noted, in drafting the statute, Congress already included a heightened intent standard. For example, § 1831 requires the government to prove that the defendant intended or knew his actions would benefit a foreign government, foreign instrumentality, or foreign agent. *See generally*

Chung, 659 F.3d at 828 (discussing intent standard). The information must in fact be a trade secret (unless, as discussed in Section B.6. of this Chapter, attempt or conspiracy is charged). Additionally, the government must show that the defendant knowingly stole, or without authorization appropriated, took, carried away, possessed or concealed, or by fraud, artifice, or deception obtained trade secret information.

Under §1832, the government must prove that the defendant intended "to convert a trade secret ... to the economic benefit of anyone other than the owner" of the trade secret, "intending or knowing that the offense will, injure any owner of that trade secret," and "knowingly" misappropriated the trade secret information. As with § 1831, the information must in fact be a trade secret (unless attempt or conspiracy is charged), and the government must show that the defendant knowingly stole, or without authorization appropriated, took, carried away, possessed or concealed, or by fraud, artifice, or deception obtained trade secret information.

Under the last element (knowingly stole a trade secret), the government must show that the defendant knowingly misappropriated (e.g., possessed or concealed) information belonging to the trade secret owner; in other words, the defendant knowingly misappropriated property belonging to someone else without permission.

A recent district court opinion following a bench trial of a § 1831 case directly addressed the *mens rea* requirement of the EEA, concluding that the Government must prove that the defendant knew the information he misappropriated was actually a trade secret (which included proof of the defendant's knowledge of the sub-elements of the definition of a trade secret). *See Chung*, 633 F. Supp. 2d 1134 (bench trial conviction of a former Boeing employee of economic espionage with the intent to benefit a foreign government). The government asserted that the term "knowingly" modified only the active conduct elements of the offense ("receives, buys, or possesses") and did not require proof that the defendant knew the information at issue fell within the precise statutory definition of a trade secret, as set forth in the EEA. *Id.*

Acknowledging that the statutory language of § 1831(a)(3) is not explicitly clear whether the word "knowingly" modifies "trade secret," the court concluded that canons of statutory construction supported an interpretation requiring proof that the defendant knew the information he received, possessed

or bought was a trade secret. *Id.* at 1145. However, the court found that this was not a difficult element to satisfy, at least based on the facts presented in the *Chung* case:

> A defendant charged with economic espionage will necessarily have some understanding of the measures that have been taken to protect the information he possesses. He will know whether the facility he acquired the information from was gated. He will know if the information in his possession has proprietary, trade secret, or classified markings. If he is an employee, he will know his company's policy about whether documents can be taken home. The Government need not prove that a defendant knew all of the security measures taken to protect the information. Likewise, proving that a defendant charged with economic espionage knows that the information he possesses has economic value is not exceedingly difficult. A spy does not deal in worthless or readily ascertainable information.

Id. at 1145-46. Moreover, the court was clear that this element did not require the government to prove that the defendant knew his conduct was illegal. *Id.*

In contrast to the district court, however, in considering the sufficiency of the evidence, the Ninth Circuit did not require the defendant to know that the information he misappropriated was actually a trade secret. *See Chung*, 659 F.3d at 824-28. Rather, the Ninth Circuit concluded that the evidence was sufficient to support the trial conviction and that a trade secret had been established.

Based on the statute and legislative history, noted above, the government should be able to satisfy the "knowingly" requirement by showing that the defendant knew or had a firm belief that the information was proprietary; was valuable to its owner because it was not generally known to the public; and that its owner had taken measures to protect it, that is, the information had the attributes of a trade secret described in § 1839(3). *See* 18 U.S.C. § 1839(3); H.R. Rep. No. 104-788, at 12 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4030-31 ("the government must prove that the defendant's actions were not authorized by the nature of his or her relationship to the owner of the property and that the defendant knew or should have known that fact"); *Krumrei*, 258 F.3d at 539 ("defendant need not have been aware of the particular security measures taken by" the trade secret owner; "Regardless of his knowledge of

those specific measures, defendant knew the information was proprietary."); *cf. Genovese*, 409 F. Supp. 2d at 258 (discussing alleged circumstances that would indicate that EEA defendant knew the information was proprietary). Evidence that the defendant was aware of confidentiality agreements or policies concerning the information, proprietary markings and other security measures taken by the information's owner will help to satisfy this element. On the other hand, a person cannot be prosecuted under the EEA if "[a] person [took] a trade secret because of ignorance, mistake, or accident." 142 Cong. Rec. 27,117 (1996). Nor could he be prosecuted if "he actually believed that the information was not proprietary after [he took] reasonable steps to warrant such belief." *Id.*

4. Additional 18 U.S.C. § 1831 Element: Intent to Benefit a Foreign Government, Foreign Instrumentality, or Foreign Agent

Under 18 U.S.C. § 1831, the second *mens rea* requirement is that the defendant intended or knew that the offense would "benefit" a "foreign government, foreign instrumentality, or foreign agent." Under this section, there is no requirement to show the government's role to obtain the trade secret (even where such proof may be present); the focus is on the defendant's knowledge that the offense would benefit or intent to benefit the "foreign government, foreign instrumentality, or foreign agent." *See generally Chung*, 659 F.3d at 828 ("Unlike the foreign agent count, which required evidence of a foreign government's direction or control, criminal liability under the EEA may be established on the basis of Defendant's intent alone."; concluding that the defendant's intent was shown by his supplying technical information in response to requests for such information from Chinese officials and by his continuing possession of trade secret materials relating to the space shuttle and the Delta IV Rocket), *cert. denied*, _ U.S. _ (2012). Consequently, normally evidence regarding the conduct or intent of the foreign government or its officials is not a requirement to establish a violation under § 1831.

A "foreign instrumentality" is "any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government." 18 U.S.C. § 1839(1). A "foreign agent" is "any officer, employee, proxy, servant, delegate, or representative of a foreign government." 18 U.S.C. § 1839(2). Thus, the government must show that the defendant knew or had a firm belief that misappropriation would benefit an entity controlled by a foreign government.

If this "entity" is not a government entity per se, such as a business, there must be "evidence of foreign government sponsored or coordinated intelligence activity" with the entity. 142 Cong. Rec. 27,116 (1996).

The "benefit" to the foreign entity should be interpreted broadly. As the House Report clarified:

> The defendant did not have to intend to confer an economic benefit to the foreign government, instrumentality, or agent, to himself, or to any third person. Rather, the government need only prove that the actor intended that his actions in copying or otherwise controlling the trade secret would benefit the foreign government, instrumentality, or agent in any way. Therefore, in this circumstance, benefit means not only an economic benefit but also reputational, strategic, or tactical benefit.

H.R. Rep. No. 104-788, at 11 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4030.

The requirement that the benefit accrue to a foreign government, instrumentality, or agent should be analyzed very carefully. To establish that the defendant intended to benefit a "foreign instrumentality," the government must show that the entity was "*substantially* owned, controlled, sponsored, commanded, managed, or dominated by a foreign government." 18 U.S.C. § 1839(1) (emphasis added). The EEA does not define "substantially," but the legislative history clarifies that the prosecution need not prove complete ownership, control, sponsorship, command, management, or domination:

> Substantial in this context, means material or significant, not technical or tenuous. We do not mean for the test of substantial control to be mechanistic or mathematical. The simple fact that the majority of the stock of a company is owned by a foreign government will not suffice under this definition, nor for that matter will the fact that a foreign government only owns 10 percent of a company exempt it from scrutiny. Rather the pertinent inquiry is whether the activities of the company are, from a practical and substantive standpoint, foreign government directed.

142 Cong. Rec. 27,116 (1996).

Thus, § 1831 does not apply to a defendant who intended who knew that the offense would benefit a foreign corporation not substantially controlled by a foreign government. *Id*. In such an instance, however, the defendant could still be properly charged under 18 U.S.C. § 1832.

Before charges may be filed under § 1831, the Counterespionage Section (CES), National Security Division (NSD) must approve. The USAM provides:

> The United States may not file a charge under 18 U.S.C. § 1831 of the Economic Espionage Act (hereinafter the "EEA"), or use a violation under § 1831 of the EEA as a predicate offense under any other law, without the approval of the Assistant Attorney General for the [National Security Division] (or the Acting official if a position is filled by an acting official). Responsibility for reviewing requests for approval of charges to be brought under § 1831 rests with the Counterespionage Section which shall obtain approval from the Assistant Attorney General for the [National Security Division]."

USAM 9-59.100; *see also* USAM 9-2.400.

CCIPS is available to assist on legal or evidence gathering questions. DOJ has strongly encouraged prosecutors to consult with CCIPS prior to filing § 1832 charges, under USAM 9-59.110 ("Prosecutors are strongly urged to consult with the Computer Crime and Intellectual Property Section before initiating prosecutions under 18 U.S.C. § 1832"), and the Memorandum from the Attorney General, Renewal of Approval Requirement Under The Economic Espionage Act of 1996, (March 1, 2002) ("I strongly urge prosecutors to consult with the Computer Crime and Intellectual Property Section (CCIPS) regarding § 1832 prosecutions prior to filing charges."). CCIPS has provided assistance on a number of cases raising trade secret and economic espionage act issues.

For questions concerning charges under § 1831, contact the Department's Counterespionage Section, within the National Security Division, at (202) 514-1187, or concerning other related issues in trade secret cases, CCIPS at (202) 514-1026.

5. Additional 18 U.S.C. § 1832 Elements

a. Economic Benefit to a Third Party

Under 18 U.S.C. § 1832, the government must prove that the defendant's misappropriation was intended for the "economic benefit of anyone other than the owner thereof." 18 U.S.C. § 1832(a). The recipient of the intended benefit can be the defendant, a competitor of the victim, or some other person or entity.

One who misappropriates a trade secret but who does not intend for anyone to gain economically from the theft cannot be prosecuted under 18 U.S.C. § 1832. This requirement differs from foreign-government economic espionage under 18 U.S.C. § 1831, for which the economic or non-economic nature of the misappropriation is immaterial. *Compare* 18 U.S.C. § 1831(a) *with* § 1832(a).

b. Intent to Injure the Owner of the Trade Secret

Beyond demonstrating in a § 1832 case that the defendant both knew that the information he took was proprietary and that he intended the misappropriation to economically benefit someone other than the rightful owner, the government must also prove that the defendant intended to "injure" the owner of the trade secret. *See* 18 U.S.C. § 1832(a). This provision "does not require the government to prove malice or evil intent, but merely that the actor knew or was aware to a practical certainty that his conduct would cause some disadvantage to the rightful owner." H.R. Rep. No. 104-788, at 11-12 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4030.

By definition, for a trade secret to have value, it must confer a commercial advantage to its owner. *See* 18 U.S.C. § 1839(3)(B); H. R. Rep. No. 104-788, at 4. The trade secret loses its value once it is disclosed to another person for the recipient's benefit. *See* H. R. Rep. No. 104-788, at 11 ("[M]isappropriation effectively destroys the value of what is left with the rightful owner.").

Absent direct evidence of an individual's intent or knowledge that the trade secret's owner would be injured by the theft, such as an admission, intent to injure will typically be shown through the circumstances around the individual's conduct. Such circumstantial evidence of intent to injure could include, among other things: lying to supervisors about post-employment plans; taking steps to cover one's tracks, such as destroying an employer's original files after making copies for use at a new job; disclosing the victim's trade secret information to

a competitor; using the victim's trade secret information while working for a competitor; and directing business to a new employer while still employed by the victim. *See, e.g., United States v. Martin*, 228 F.3d 1, 12 (1st Cir. 2000) (intent to injure shown by "plan of competition").

As discussed in greater detail in Section C.1.a., below, lack of intent to injure is a common defense that may pose particular challenges in cases where a departing employee is apprehended or searched before he or she has the opportunity to disclose the former employer's trade secrets to the new employer.

c. Product or Service Used or Intended for Use in Interstate or Foreign Commerce

On a charge of economic espionage under 18 U.S.C. § 1832, the government must prove that the trade secret was "related to a product or service used or intended for use in interstate or foreign commerce." 18 U.S.C. § 1832 (as amended by the Theft of Trade Secrets Clarification Act, Pub. L. No. 112-236, § 2, 126 Stat. 1627 (2012)); *compare* 18 U.S.C. § 1831 (containing no comparable language).

Because the nexus to interstate or foreign commerce was likely included to provide a basis for federal jurisdiction, the government does not have to prove that they defendant knew that the trade secret was related to a product or service used or intended for use in interstate or foreign commerce. The statute's plain text confirms this. The jurisdictional language quoted above is set off in the statute by commas to qualify which types of trade secrets fall under the statute. It precedes the word "knowingly," thus putting it outside the elements the government must prove the defendant knew.

The phrase "a product or service used or intended for use in interstate or foreign commerce" includes trade secrets developed for existing products and for future products. In the case of an existing product, this nexus can usually be satisfied by evidence of the trade secret's connection to the current product and the product's current or potential interstate or foreign sales.

By contrast, for products still being developed, § 1832 merely requires proof that the trade secret was "related to a product or service … intended for use in interstate or foreign commerce." 18 U.S.C. § 1832(a). A defendant might try to argue that a product still in the research and development stage is not yet "intended for use in … interstate commerce," 18 U.S.C. § 1832, because the prototype itself is not "intended" for sale. But this argument would

withhold the EEA's protection when it was most needed. The research and development phase is often when a trade secret is most valuable. Once the final product embodying the trade secret is released to the public, the trade secret's value can be lost because of its availability to competitors who can examine the product legitimately and obtain or deduce the trade secret for themselves.

In considering the interstate commerce element of § 1832 (prior to the 2012 amendment), the court in *United States v. Yang* held that a patent application had a sufficient nexus to interstate commerce because it involved a product that generated $75-100 million in sales the previous year and it was related to products produced and sold in the United States and Canada; and also because the victim also had sought patents for the product in Europe. 281 F.3d 534, 551 & n.4 (6th Cir. 2002).

Prior to December 28, 2012, the "interstate commerce" element of § 1832—which required that the trade secret in question be "related to or included in a product that is produced for or placed in interstate or foreign commerce"—was arguably narrower than the amended language in two ways. First, the previous language required a connection to a "product." Second, it required that the product be "produced for or placed in" interstate commerce, rather than be related to a product or service that is "used or intended for use in" interstate or foreign commerce.

In *United States v. Aleynikov*, the Second Circuit further narrowed what was considered a product that is "produced for or placed in" interstate comment. 676 F.3d 71 (2d Cir. 2012).

In *Aleynikov*, a former Goldman Sachs programmer was convicted of violating 18 U.S.C. § 1832 for stealing trade secret computer source code related to Goldman Sachs' high-frequency trading (HFT) platform. *Id.* at 73. HFT involves using computer algorithms to quickly analyze market movements and execute large numbers of stock trades in order to exploit tiny price discrepancies. *Id.* Goldman Sachs used the software code at issue in *Aleynikov* to facilitate the flow of information through its HFT system and to monitor system performance. *Id.* at 74.

The district court denied defendant's motion to dismiss, in which he argued that the high-frequency trading system source code trade secret was not sufficiently "related to or included in a 'product' that is 'produced for or placed in interstate and foreign commerce.'" *United States v. Aleynikov*, 737 F. Supp. 2d 173 (S.D.N.Y. 2010), *rev'd*, 676 F.3d 71 (2d Cir. 2012). Although

the statute did not define the term "product," the district court concluded that "[t]he ordinary meaning of 'product' is something that is the result of human or mechanical effort or some natural process." *Id.* at 178. The court explained that the misappropriated source code satisfied this definition and further, was expressly developed to enable the company to engage in interstate and foreign commerce. *Id.* at 179.

On appeal, the Second Circuit reversed the district court's decision. Noting that Goldman Sachs had no intention of selling or licensing its HFT software to anyone else, the Second Circuit concluded that "because the HFT [high-frequency trading] system was not designed to enter or pass in commerce, or to make something that does, Aleynikov's theft of source code relating to that system was not an offense under the EEA." *Aleynikov*, 676 F.3d at 82. In construing the statute, the Second Circuit found that in order to give meaning to both "produced for" and "placed in" interstate commerce, the product at issue has to be either sold (i.e., placed in) in interstate commerce or produced for such placement but for its stage of development (e.g., prototypes). *Id.* at 80-81.

In response to the Second Circuit's decision in *Aleynikov*, the Theft of Trade Secrets Clarification Act made clear that Congress intends 18 U.S.C. § 1832 to cover a broader array of trade secret thefts than the Second Circuit's narrow reading of the pre-2012 amendment version of the statute would allow. *See* 158 Cong. Rec. S6978 (daily ed. Nov. 27, 2012), 2012 WL 5932548 ("The clarifying legislation that the Senate will pass today corrects the [*Aleynikov*] court's narrow reading to ensure that our federal criminal laws adequately address the theft of trade secrets related to a product or service used in interstate commerce.") (statement of Sen. Leahy). This 2012 amendment changed § 1832 to read as follows:

> Whoever, with intent to convert a trade secret, that is related to ~~or included in a product that is produced for or placed in~~ a product or service used in or intended for use in interstate or foreign commerce, …

This new statutory language contains two primary changes. First, it specifically applies to both products and services. Second, it replaces the requirement that the product be "produced for or placed in" interstate commerce (which the Second Circuit in *Aleynikov* interpreted to require that the trade secret information itself either enter or pass into commerce, or be used to "make

something that does") with a broader definition that requires only that the trade secrets at issue be related to a product or service that is "used in or intended for use in" interstate or foreign commerce.

6. Attempts and Conspiracies, Including the Impossibility Defense

The EEA punishes attempts and conspiracies to misappropriate trade secrets. 18 U.S.C. §§ 1831(a)(4)-(5), 1832(a)(4)-(5). For an attempt, the defendant must (1) have the intent needed to commit a crime defined by the EEA, and (2) perform an act amounting to a "substantial step" toward the commission of that crime. *Hsu*, 155 F.3d at 202. For a conspiracy, the defendant must agree with one or more people to commit a violation, and one or more of the co-conspirators must commit an overt act to effect the object of the conspiracy. 18 U.S.C. §§ 1831(a)(5), 1832(a)(5). *See generally Chung*, 659 F.3d at 828-29 (listing elements).

To convict a defendant under the EEA of attempt or conspiracy, however, the government is not required to prove that the information the defendant sought actually constituted a trade secret. *Hsu*, 155 F.3d at 204.

In *Hsu*, the defendants were charged with attempting and conspiring to steal the techniques for manufacturing an anti-cancer drug from Bristol-Meyers Squibb. The district court compelled the government to disclose to the defendants the trade secrets at issue, on the grounds that the defendants were entitled to demonstrate that the materials were not trade secrets in fact. *United States v. Hsu*, 982 F. Supp. 1022, 1024 (E.D. Pa. 1997). On interlocutory appeal, the Third Circuit disagreed, holding that to prove an attempt or conspiracy under the EEA, the government need not prove the existence of an actual trade secret, but, rather, that the defendants *believed* that the information was a trade secret—regardless of whether the information was truly a trade secret or not—and that they conspired in doing so. *Hsu*, 155 F.3d at 203 ("the government need not prove that an actual trade secret was used …, because a defendant's culpability for a charge of attempt depends only on 'the circumstances as he believes them to be,' not as they really are"). Thus, to prove an attempt, the government need only prove "beyond a reasonable doubt that the defendant sought to acquire information which he or she believed to be a trade secret, regardless of whether the information actually qualified as such." *Id.*

In reaching its conclusion the Third Circuit rejected the defendants' contention that the government had to disclose the trade secrets so the defendants could prepare a potential defense of legal impossibility. Although

elsewhere the Third Circuit generally allowed the common-law defense of legal impossibility in cases charging attempt, it found that the EEA clearly showed Congress's intent to foreclose an impossibility defense. *Hsu,* 155 F.3d at 202 ("[T]he great weight of the EEA's legislative history evinces an intent to create a comprehensive solution to economic espionage, and we find it highly unlikely that Congress would have wanted the courts to thwart that solution by permitting defendants to assert the common law defense of legal impossibility."). The court found it significant that "[t]he EEA was drafted in 1996, more than twenty-five years after the National Commission on Reform of the Federal Criminal Laws had concluded that the abolition of legal impossibility was already 'the overwhelming modern position.'" *Id*. Lastly, the court noted that if legal impossibility were "a defense to the attempted theft of trade secrets, the government would be compelled to use actual trade secrets during undercover operations." *Id*. This would "have the bizarre effect of forcing the government to disclose trade secrets to the very persons suspected of trying to steal them, thus gutting enforcement efforts under the EEA." *Id*. Therefore, the court held that "legal impossibility is not a defense to a charge of attempted misappropriation of trade secrets in violation of 18 U.S.C. § 1832(a)(4)." *Id*.

Nor is legal impossibility a defense to a charge of conspiracy to violate the EEA. Because the basis of a conspiracy charge is the "conspiratorial agreement itself and not the underlying substantive acts," the impossibility of achieving the conspiracy's goal is irrelevant. *See Hsu*, 155 F.3d at 203 (citing *United States v. Jannotti*, 673 F.2d 578, 591 (3d Cir.1982) (en banc)); *see also United States v. Wallach*, 935 F.2d 445, 470 (2d Cir. 1991)*; United States v. LaBudda*, 882 F.2d 244, 248 (7th Cir. 1989); *United States v. Petit*, 841 F.2d 1546, 1550 (11th Cir. 1988); *United States v. Everett*, 692 F.2d 596, 599 (9th Cir. 1982).

Hsu's reasoning has been adopted by the Sixth Circuit in *United States v. Yang*, 281 F.3d 534, 541-45 (6th Cir. 2002); the Seventh Circuit in *United States v. Lange*, 312 F.3d 263, 268-69 (7th Cir. 2002); and the First Circuit in *United States v. Martin*, 228 F.3d 1, 13 (1st Cir. 2000).

C. Defenses

1. Common Defenses

a. Lack of Intent to Convert a Trade Secret

A common defense in both civil trade secret misappropriation and criminal EEA cases is that the defendant did not intend to convert a trade secret for the benefit of someone other than its owner, but intended only to use publicly available information or general skills and knowledge acquired throughout the defendant's career. The defendant's intent to convert the trade secret is an essential element of the offense; absent proof of wrongful intent beyond a reasonable doubt, the defendant will be acquitted. *See, e.g., United States v. Shiah*, No. SA CR 06-92 (C.D. Cal. Feb. 19, 2008) (unpublished), *available at* http://court.cacd.uscourts.gov/CACD/RecentPubOp.nsf/ecc65f191f28f59b8825728f005ddf4e/37d207fcb9587a30882573f400620823/$FILE/SACR06-92DOC.pdf. This defense is rooted in Congress' stated purpose to differentiate between trade secrets, which are the subject matter of the EEA, and a person's general skills and knowledge, which are not. The House Report states that the EEA does not apply "to individuals who seek to capitalize on the personal knowledge, skill, or abilities they may have developed" in moving from one job to another. H. R. Rep. No. 104-788, at 7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4026. "The statute is not intended to be used to prosecute employees who change employers or start their own companies using general knowledge and skills developed while employed." *Id.* "It is not enough to say that a person has accumulated experience and knowledge during the course of his or her employ. Nor can a person be prosecuted on the basis of an assertion that he or she was merely exposed to a trade secret while employed. A prosecution that attempts to tie skill and experience to a particular trade secret should not succeed unless it can show that the particular material was stolen or misappropriated." 142 Cong. Rec. 27, 117 (1996); *see also United States v. Martin*, 228 F.3d 1, 11 (1st Cir. 2000) (emphasis in original) (Section 1832(a) "was not designed to punish competition, even when such competition relies on the know-how of former employees of a direct competitor. It *was*, however, designed to prevent those employees (and their future employers) from taking advantage of confidential information gained, discovered, copied, or taken while employed elsewhere."); *Shiah*, No. SA CR 06-92 (same).

A defendant successfully invoked this defense against § 1832 charges during a bench trial in *United States v. Shiah*, No. SA CR 06-92. The defendant

had been a product line manager at Broadcom, a semi-conductor company, for approximately two-and-a-half years, where he had been exposed to technical, marketing and price information on a variety of Broadcom products. Shortly after receiving a negative performance evaluation, the defendant applied for and was offered a similar position with a direct competitor. After applying for the new job, but before tendering his resignation, the defendant went about collecting electronic documents concerning matters he had worked on at Broadcom. On the same day he intended to give notice of his resignation, the defendant copied 4,700 files from his Broadcom laptop onto an external hard drive.

At the defendant's exit interview, Broadcom's general counsel told the defendant that he was forbidden from disclosing Broadcom's confidential information, which he said included technical documents, pricing lists and a wider range of business information. The defendant was not shown a copy of the confidentiality agreement he had signed when he started working at Broadcom. After he began working for the competitor, the defendant accessed several of the electronic Broadcom files he had kept while performing his new job.

At trial, the defendant claimed he did not intend to use or disclose any of the confidential Broadcom information contained in the thousands of files he copied onto his external hard drive. Instead, he claimed he would rely on his own internal filter to use only the non-confidential and publicly available information in the thousands of documents he had copied. He considered this information to be part of his "tool kit" of information he had developed during the course of his career in the computer device industry. In support of this argument, he pointed to evidence he had copied thousands of documents from his prior employer before joining Broadcom. The defendant further testified that of the Broadcom documents he accessed after leaving the company, he used only the non-confidential information from them concerning aggregate industry information.

Although the trial court found that the defendant's pattern of access to the Broadcom files while at his new job was "suspicious," and that the evidence indicated that it was more likely than not that defendant did intend to convert trade secrets (which would have satisfied a *preponderance* standard), it concluded that the government fell "just short" of proving the defendant's intent to convert the trade secrets *beyond a reasonable doubt* because his alternative explanation for his conduct was sufficient to create a reasonable doubt. The

court ultimately found that the defendant's claimed "tool kit" defense was consistent with the defendant's past practices and with his wholesale copying of files on his Broadcom laptop. The court also relied on the facts that many of the files that the defendant copied were marketing documents that contained both trade secret and non-confidential information and that there was no evidence that the confidential portions of the documents were disclosed to the defendant's new co-workers. The court also found the defendant's efforts to acquire certain Broadcom documents before leaving the company were equally consistent with defendant's claimed efforts to address a point of criticism in his recent performance evaluation that he lacked detailed product knowledge as they were with a malicious intent.

The *Shiah* case underscores the importance of developing evidence of intent to convert. Certainly the best evidence of such intent is direct evidence of disclosure of the trade secrets to the new employer or other third parties. However, evidence of disclosure is often not available when a defendant is searched or arrested shortly after leaving his or her former employer with a treasure trove of trade secrets in hand. Therefore, it will be necessary to develop circumstantial evidence of the defendant's behavior by looking to his conduct and actions around the time of the misappropration.

b. Information is Not a Trade Secret

i. Owner Failed to Take Reasonable Measures to Protect Secrecy

Another common defense to EEA charges is that the trade secret's owner failed to take reasonable measures to protect the secrecy of the information at issue. As discussed in Section B.3.a.v. of this Chapter, the government is not required to prove that the victim took all available measures to keep its information secret. The standard is whether measures the owner took were reasonable under the circumstances.

Although there are no reported EEA cases in which this defense was successful, the *United States v. Shiah* case provides detailed insight into the factors at least one trial court considered when weighing this element. Although the court ultimately found that the government had satisfied its burden beyond a reasonable doubt, it expressed concern that the measures taken by the trade secret owner "were barely sufficient to qualify as reasonable." *Shiah*, No. SA CR 06-92, at 31. The court focused its concerns not on the physical or electronic security measures taken by Broadcom, but on its practices toward its employees. For example, the court found that Broadcom had not provided

the defendant with a copy of his confidentiality agreement after he signed it, and did not explain the meaning of the agreement to him both at the outset of his employment or during his exit interview. The court was also critical of Broadcom's failure to provide regular training to its employees on protecting confidential information, and the absence of a comprehensive system in place for designating which documents were and which documents were not confidential. Finally, the court criticized Broadcom's failure to examine the defendant's computer immediately upon his departure.

Despite these complaints, the court found that the deficiencies in the trade secret owner's practices were not so extensive as to qualify as unreasonable, because, as a whole, the company's measures were generally effective. This conclusion was supported by evidence that Broadcom employees generally understood what types of information the company considered to be confidential, as well as evidence that the company had a reputation of being "stingy" with its data protection. *Id.* at 36. As the reasonable measures element is based on what steps were taken to keep the information secret from the public, the court correctly noted that the owner is not required to keep the information secret from the trade secret owner's own employees, because otherwise "'no one could do any work.'" *Id.* at 32 (quoting *Lange*, 312 F.3d at 266). Nevertheless, the court stated that a company could fall short if it failed to take reasonable measures to prevent a departing employee from taking trade secrets with him upon termination.

The *Shiah* case, and the cases discussed in Section B.3.a.v. above suggest that this defense will be successful only in situations where the victim's security environment is so lax that disclosures of confidential information are frequent occurrences, or where a company fails to employ a combination of technical, physical and contractual tools to protect its information.

ii. Information is Not Secret

The government bears the burden of proving, beyond a reasonable doubt, that the alleged trade secrets derived economic value from not being generally known or readily ascertainable to the public through proper means. Defendants will often try to inject doubt into this element by presenting evidence that the alleged trade secrets were generally known to persons in the industry or that they had been publicly disclosed. This is often done through a defense expert witness who is familiar with the industry or the technology at issue.

In addition, the defendant may argue that the victim has publicly disclosed some aspect of the alleged trade secret. For this reason, the prosecutor and investigator should ascertain early on whether the purported trade secret was ever disclosed, in whole or in part, and to what extent those disclosures affect the information's status as a trade secret. These issues are discussed further in Donald M. Zupanec, Annotation, *Disclosure of Trade Secret as Abandonment of Secrecy*, 92 A.L.R.3d 138 (2012) and 1 Roger M. Milgrim, *Milgrim on Trade Secrets* §§ 1.05-1.06. The following is an overview.

- **Disclosure Through the Patent and Copyright Processes**

Information that has been disclosed in a patent application can nevertheless qualify as a trade secret between the time of the application's submission and the patent's issuance, as long as the patent application itself is not published by the patent office. *Scharmer v. Carrollton Mfg. Co.*, 525 F.2d 95, 99 (6th Cir. 1975) (citing *Grant v. Raymond*, 31 U.S. 218, 242 (1832)); *see generally Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 482-93 (1974) (noting distinct intellectual property roles served by patents and trade secrets). The patented process or device is no longer a trade secret once the application is published or the patent is issued because publication of the application or patent makes the process publicly available for all to see. *Id.* at 485 (citing 35 U.S.C. § 122 and 37 C.F.R. § 1.14(b)); *see also On-Line Techs. v. Perkin-Elmer Corp.*, 253 F. Supp. 2d 313, 323-27 (D. Conn. 2003). Patent applications filed in the United States after November 29, 2000, are typically published after 18 months. At the beginning of the investigation, the prosecutor and investigator should ask the victim for copies of all published patent applications and issued patents covering the subject matter of the trade secret information to determine whether it has been disclosed. See Chapter VII of this Manual.

A subsequent refinement or enhancement to the patented technology may be a trade secret if it is not reasonably ascertainable from the published patent itself. *See United States v. Hsu*, 185 F.R.D. 192, 200 (E.D. Pa. 1999).

Even where some elements are publicly known through a patent application, trade secret status may be found where non-public elements are included. *See, e.g., Penalty Kick Mgmt. Ltd. v. Coca Cola Co.*, 318 F.3d 1284, 1291 (11th Cir. 2003) (concluding that beverage label marketing and production process qualified as a trade secret since "nothing in the ... patent application dealt with the production elements used to produce" the labels).

Substantially the same analysis applies to information that has been submitted to the United States Copyright Office for registration. Submitting material to the Copyright Office can render it open to public examination and viewing, thus destroying the information's value as a trade secret, unless the material is submitted under special procedures to limit trade secret disclosure. *See Tedder Boat Ramp Sys., Inc. v. Hillsborough County, Fla.*, 54 F. Supp. 2d 1300, 1303-04 (M.D. Fla. 1999); *Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc.*, 923 F. Supp. 1231, 1255 n.28 (N.D. Cal. 1995); 1 *Milgrim on Trade Secrets* § 1.06[6]-[9]. *But see Compuware Corp. v. Serena Software Int'l, Inc.*, 77 F. Supp. 2d 816 (E.D. Mich. 1999) (holding that material could continue to be a trade secret even after its owner submitted it to the Copyright Office without redaction, because the owner had taken other steps to keep it secret and there was no evidence that it had become known outside the owner's business).

- **Disclosure Through Industry Publications or Conferences**

Information can also lose protection as a trade secret through accidental or intentional disclosure by an employee at a conference or trade show, or in technical journals or other publications. *See, e.g.*, *Mixing Equip. Co. v. Philadelphia Gear, Inc.*, 436 F.2d 1308, 1311 n.2 (3d Cir. 1971) (holding that industrial mixing equipment charts and graphs lost trade secret status through publication in trade journals).

- **Disclosure to Licensees, Vendors, and Third Parties**

Information that has been disclosed to licensees, vendors, or third parties for limited purposes can remain a trade secret under some circumstances, including covering the disclosures by a non-disclosure agreement. *See, e.g.*, *Lange*, 312 F.3d at 266; *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 177 (7th Cir. 1991). For the security measures the trade secret owner should take to maintain secrecy during those disclosures, see Section B.3.a.v., of this Chapter.

- **Disclosure Through Internet Postings**

A trade secret can lose its protected status after it is posted anonymously on the Internet, even if the trade secret was originally gathered through improper means. *See Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc.*, 923 F. Supp. 1231 (N.D. Cal. 1995). If the Internet posting causes the information to fall into the public domain, a person who republishes the

information is not guilty of misappropriating a trade secret, even if he knew that the information was originally acquired by improper means. *DVD Copy Control Ass'n Inc. v. Bunner*, 10 Cal. Rptr. 3d 185, 194 (Cal. Ct. App. 2004). "[T]hat which is in the public domain cannot be removed by action of the states under the guise of trade secret protection." *Id.* at 195.

Disclosure over the Internet may not always strip away a trade secret's protection automatically. For example, in *United States v. Genovese*, the court held that a trade secret could retain its secrecy despite a brief disclosure over the Internet: "[A] trade secret does not lose its protection under the EEA if it is temporarily, accidentally or illicitly released to the public, provided it does not become 'generally known' or 'readily ascertainable through proper means.'" 409 F. Supp. 2d 253, 257 (S.D.N.Y. 2005) (citing 18 U.S.C. § 1839(3)(B)). Publication on the Internet may not destroy the trade secret's status "if the publication is sufficiently obscure or transient or otherwise limited so that it does not become generally known to the relevant people, i.e., potential competitors or other persons to whom the information would have some economic value." *DVD Copy Control Ass'n Inc.*, 10 Cal. Rptr. 3d at 192-93.

- **Disclosure During Law Enforcement Investigations**

Disclosures to the government to assist an investigation or prosecution of an EEA case should not waive trade secret protections. *See United States v. Yang*, 1999 U.S. Dist. LEXIS 7130 (N.D. Ohio Mar. 18, 1999) (holding that victim's disclosure of trade secret to government for use in a sting operation under oral assurances that the information would not be used or disclosed for any purpose unrelated to the case did not vitiate trade secret status). Disclosure to the government is essential for the investigation and prosecution of illegal activity and is expressly contemplated by the EEA. First, 18 U.S.C. § 1833(2) specifically encourages disclosures to the government, stating: "[the EEA] does not prohibit ... the reporting of a suspected violation of law to any governmental entity of the United States ... if such entity has lawful authority with respect to that violation." Second, 18 U.S.C. § 1835 authorizes the court to "enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure ... and all other applicable laws." *See also infra* Section D. of this Chapter. Section 1835 gives "a clear indication from Congress that trade secrets are to be protected to the fullest extent during EEA litigation." *Hsu*, 155 F.3d at 197. Together, these sections demonstrate Congress's intent to encourage the reporting of an EEA violation.

Laws other than the EEA similarly limit the Department of Justice's disclosure of trade secrets without the consent of the trade secret owner or the express written authorization of senior officials at the Department. *See, e.g.*, 28 C.F.R. § 16.21 (2012).

Information does not lose its status as a trade secret if the government discloses it to the defendant as "bait" during a sting operation. *See United States v. Hsu*, 185 F.R.D. 192, 199 (E.D. Pa. 1999). "To hold that dangling such bait waives trade secret protection would effectively undermine the Economic Espionage Act at least to the extent that the Government tries ... to prevent an irrevocable loss of American technology before it happens." *Id.*

- **Disclosure by the Original Misappropriator or His Co-Conspirators**

The person who originally misappropriates a trade secret cannot immunize himself from prosecution by disclosing it into the public domain. Although disclosure of a trade secret may cause it to lose trade-secret status *after* the disclosure, disclosure does not destroy trade-secret status retroactively. Consequently, one who initiates the disclosure may be prosecuted, whereas one who distributes the information post-disclosure may not, unless he was working in concert with the original misappropriator. *Cf. Underwater Storage, Inc. v. United States Rubber Co.*, 371 F.2d 950, 955 (D.C. Cir. 1966) ("We do not believe that a misappropriator or his privies can 'baptize' their wrongful actions by general publication of the secret."); *Religious Tech. Ctr.*, 923 F. Supp. at 1256.

2. Parallel Development

The essence of the parallel development defense is that the defendant independently, through its own efforts, developed the same information as the putative victim, without access to the victim's trade secrets. Indeed, the owner of a trade secret, unlike the holder of a patent, does not have "an absolute monopoly on the information or data that comprises a trade secret." 142 Cong. Rec. 27,116 (1996). Other companies and individuals have the right to discover the information underlying a trade secret through their own research and hard work; if they do, there is no misappropriation under the EEA. *Id.* Of course, this defense would prove ineffective where direct evidence of the defendant's acquisition of the trade secrets from the victim exists.

3. Reverse Engineering

Similarly, a person may legally discover the information underlying a trade secret by "reverse engineering," that is, the practice of taking apart something that was legally acquired to determine how it works or how it was made or manufactured. *See, e.g.*, *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974) (holding that the law does not protect the owner of a trade secret from "discovery by fair and honest means, such as by independent invention, accidental disclosure, or by so-called reverse engineering"); *ConFold Pac., Inc. v. Polaris Indus.*, 433 F.3d 952, 959 (7th Cir. 2006) ("[I]t is perfectly lawful to 'steal' a firm's trade secret by reverse engineering.") (Posner, J.) (citations omitted).

Although the EEA does not expressly address when reverse engineering is a valid defense, its legislative history states that "[t]he important thing is to focus on whether the accused has committed one of the prohibited acts of this statute rather than whether he or she has 'reverse engineered.' If someone has lawfully gained access to a trade secret and can replicate it without violating copyright, patent or this law, then that form of 'reverse engineering' should be fine." 142 Cong. Rec. 27,116 (1996).

The mere fact that a particular secret *could* have been reverse engineered after a time-consuming and expensive laboratory process does not provide a defense for someone who intended to avoid that time and effort by stealing the secret, unless the information was so apparent as to be deemed "readily ascertainable," and thus not a trade secret. *See* 4 Roger M. Milgrim, *Milgrim on Trade Secrets* § 15.01[1][d][v]; *Alcatel USA, Inc. v. DGI Techs., Inc.*, 166 F.3d 772, 784-85 (5th Cir. 1999) (holding that a competitor could not assert reverse engineering defense after it had first unlawfully obtained a copy of the software and then used the copy to reverse engineer); *Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc.*, 35 F.3d 1226, 1237 (8th Cir. 1994) (stating that fact "that one 'could' have obtained a trade secret lawfully is not a defense if one does not actually use proper means to acquire the information") (citations omitted); *Telerate Sys., Inc. v. Caro*, 689 F. Supp. 221, 233 (S.D.N.Y. 1988) ("[T]he proper focus of inquiry is not whether an alleged trade secret can be deduced by reverse engineering but rather, whether improper means are required to access it.").

To counter a defense of reverse engineering, prosecutors should establish how the defendant obtained the trade secret. Proving misappropriation should refute a claim of reverse engineering.

4. Legal Impossibility

The defense of legal impossibility has largely been rejected by courts in EEA prosecutions. See Section B.6. of this Chapter.

5. Advice of Counsel

"There is no such thing as an 'advice of counsel' defense." *United States v. Urfer*, 287 F.3d 663, 665 (7th Cir. 2002) (Posner, J.) (charges of willfully injuring federal property). Rather, "if a criminal statute requires proof that the defendant knew he was violating the statute in order to be criminally liable for the violation, and it is unclear whether the statute forbade his conduct, the fact that he was acting on the advice of counsel is relevant because it bears on whether he knew that he was violating the statute." *Id.* at 666. In other words, advice of counsel is a defense only if it negates the *mens rea* needed to prove a violation.

Advice of counsel could conceivably negate an EEA defendant's *mens rea* in several ways. As is discussed in Section B.3.c. of this Chapter, the defendant cannot be convicted unless he knew that he was misappropriating a trade secret. Thus, the defendant's *mens rea* might be negated if counsel advised him either that the information in question was not a trade secret or that it was a trade secret to which he could claim ownership.

To rely on an advice of counsel claim at trial, the defendant must first provide "independent evidence showing (1) the defendant made full disclosure of all material facts to his or her attorney before receiving the advice at issue; and (2) he or she relied in good faith on the counsel's advice that his or her course of conduct was legal." *Covey v. United States*, 377 F.3d 903, 908 (8th Cir. 2004) (citations and alterations omitted); *United States v. Munoz*, 233 F.3d 1117, 1132 (9th Cir. 2000) (noting an advice of counsel instruction requires proof that the defendant "fully disclosed to his attorney all material facts and relied in good faith on the attorney's recommended course of conduct"); *see also United States v. Butler*, 211 F.3d 826, 833 (4th Cir. 2000) (same). Both elements must be shown.

Under the full disclosure requirement, the information may not be mischaracterized and all material facts must be provided. *See, e.g.*, *United States*

v. Munoz, 233 F.3d 1117, 1132 (9th Cir. 2000) (in mail fraud prosecution, defendant was not entitled to an advice of counsel instruction where, among other things, attorney's opinion letter was based on misrepresentations that investments were not advertised to general public even though defendant "honestly believed the opinion letters written by the attorneys were accurate and … did not understand the importance of not advertising … to the general public"); *United States v. Kenney*, 911 F.2d 315, 322 (9th Cir. 1990) (holding that defendant did not make a full disclosure where the defendant mischaracterized a kickback as an interest-free loan); *United States v. Conforte*, 624 F.2d 869, 877 (9th Cir. 1980) (noting a material fact is any "fact[] to which the advice pertains"); *United States v. Stirling*, 571 F.2d 708, 735 (2d Cir. 1978) (rejecting defendants' argument that attorneys failed to ask sufficiently probing questions because attorneys had "no obligation to ferret out proof of wrongdoing."). Under the good faith reliance requirement, the client must rely on the recommended course of conduct and cannot act before receiving the legal advice. *See, e.g.*, *United States v. Cheek*, 3 F.3d 1057, 1061-62 (7th Cir. 1993) (advice of counsel instruction did not apply because defendant who had been warned of illegality "merely continued a course of illegal conduct begun prior to contacting counsel"); *Conforte*, 624 F.2d at 877 (rejecting a reliance on counsel defense because, among other reasons, the defendant did not speak to his attorney until after the crimes had been committed); *see also United States v. Polytarides*, 584 F.2d 1350, 1353 (4th Cir. 1978) (good faith reliance on advice of counsel defense was not available when defendant had taken significant steps toward the illegal activity and had been warned of its illegality prior to seeking advice of an attorney).

6. Claim of Right—Public Domain and Proprietary Rights

As is discussed in Section B.3.c. of this Chapter, the defendant cannot be convicted unless he knew that the information he was misappropriating was proprietary. Thus, the defendant's *mens rea* might be negated if he believed in good faith that he had a right to use the information, either because it was in the public domain or because it belonged to him.

The former situation, information in the public domain, is discussed in Section B.3.a.iii. (discussing how disclosure affects trade secret status).

The latter situation, when the accused acts under a proprietary claim of right, can occur when two parties have a legitimate dispute over who owns the trade secret. This type of dispute is most likely to occur after the parties

developed technology together and their respective ownership interests are unclear. In these circumstances, one party's unilateral action with regard to the trade secret might precipitate a criminal referral from the other party. Such cases are rarely appropriate for criminal prosecution, especially if the putative defendant acted on the advice of counsel. See Section C.5. of this Chapter. Notwithstanding the passage of the EEA, many disputes about trade secrets are still best resolved in a civil forum.

7. The First Amendment

The First Amendment provides no defense when the defendant's speech itself is the very vehicle of the crime. *See, e.g.*, *United States v. Morison*, 844 F.2d 1057, 1068 (4th Cir. 1988) (rejecting defendant's First Amendment defense and upholding a conviction for a violation of 18 U.S.C. § 793 for stealing secret government documents, noting that "[w]e do not think that the First Amendment offers asylum ... merely because the transmittal was to a representative of the press"); *United States v. Rowlee*, 899 F.2d 1275 (2d Cir. 1990) (rejecting First Amendment defense against charges of tax evasion conspiracy). In a prosecution similar to the theft of trade secrets under the EEA, the First Amendment was held to provide no defense to a charge under 18 U.S.C. § 2314 for the interstate transportation of stolen computer files:

> In short, the court finds no support for [the defendant's] argument that the criminal activity with which he is charged ... is protected by the First Amendment. Interpreting the First Amendment as shielding [the defendant] from criminal liability would open a gaping hole in criminal law; individuals could violate criminal laws with impunity simply by engaging in criminal activities which involve speech-related activity. The First Amendment does not countenance that kind of end run around criminal law.

United States v. Riggs, 743 F. Supp. 556, 560-61 (N.D. Ill. 1990).

In most instances, if the government can establish that the defendant intended his misappropriation to benefit a third party economically, he should have a hard time claiming that his disclosure of the trade secret was protected by the First Amendment. In other words, where the defendant's motivation was pecuniary, the defendant's argument that he disclosed the trade secret as a public service or to educate the public should be significantly undermined.

See DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 194-96 (Cal. Ct. App. 2004).

Because the First Amendment does not protect speech that is criminal, the government should seek to exclude evidence regarding that defense through an appropriate motion *in limine*.

8. Void-for-Vagueness

Several defendants have challenged the EEA on grounds that it is vague or otherwise unconstitutional. Thus far, all such challenges have been rejected.

In *United States v. Hsu*, 40 F. Supp. 2d 623 (E.D. Pa. 1999), the defendant was charged with, among other things, conspiracy to steal trade secrets in violation of 18 U.S.C. § 1832(a)(5) and attempted theft of trade secrets in violation of 18 U.S.C. § 1832(a)(4). Hsu moved to dismiss, arguing that the EEA was unconstitutionally vague in numerous respects.

In denying Hsu's motion to dismiss, the court noted that a statute is not unconstitutionally vague just because "Congress might, without difficulty, have chosen 'clearer and more precise language' equally capable of achieving the end which it sought." *Hsu*, 40 F. Supp. 2d at 626 (quoting *United States v. Powell,* 423 U.S. 87, 94 (1975) (citation omitted)). Because the First Amendment was not implicated, Hsu's void-for-vagueness challenge could succeed only if the EEA were vague as applied to his conduct and as applied to "the facts of the case at hand." *Id*. at 626-27. Hsu argued that the First Amendment was implicated because the Bristol-Meyers Squibb "employee who aided the Government 'sting' operation by posing as a corrupt employee [had] a right freely to express himself and exchange information with the defendant, or with anyone else he [thought was] a potential employer." *Id.* at 627 (citations omitted). The court disagreed. It noted first that Hsu lacked standing to raise the victim's employee's purported First Amendment rights. *Id*. And even if Hsu had standing, the court said, the employee had knowingly participated in a government sting operation, not in a job interview with a potential employer. *Id*. Therefore, no First Amendment interests were implicated. *Id*.

The court also rejected Hsu's argument that the term in the pre-2012 amendment version of 18 U.S.C. § 1832 "related to or included in a product that is produced for or placed in interstate or foreign commerce is unacceptably vague." *Id*. Prior First Amendment decisions disapproving of the term "related" had no bearing on the use of "related to or included in" in the EEA, which the

court found "readily understandable to one of ordinary intelligence, particularly here, where the defendant appears to be well versed as to [the nature of the technology at issue]." *Id*.

The court also concluded that the EEA's definition of "trade secret" was not unconstitutionally vague as applied to Hsu. As to the requirement that the owner take "reasonable measures" to keep the information secret, the mere use of the word "reasonable" or "unreasonable" does not render a statute vague. *Id*. at 628. The court further noted that these terms were taken "with only minor modifications" from the Uniform Trade Secrets Act, which had been adopted in forty states and the District of Columbia and had also withstood a void-for-vagueness attack. *Id.*

Also undermining Hsu's void-for-vagueness challenge was his own knowledge of the facts at the time of the offense. Hsu knew that Bristol-Meyers Squibb had taken many steps to keep its technology secret. He had been told on several occasions that the technology was proprietary to Bristol-Meyers Squibb, could not be acquired through a license or joint venture, and could be obtained only through an allegedly corrupt employee. The court therefore held that he could not contend that the term "reasonable measures" was vague as applied to him. *Id.*

Finally, the *Hsu* court concluded that the EEA was not void for vagueness in qualifying that the information not be "generally known to" or "readily ascertainable by" the public. The court concluded that the EEA's use of those terms was problematic because "what is 'generally known' and 'readily ascertainable' about ideas, concepts, and technology is constantly evolving in the modern age." *Id.* at 630. Nonetheless, Hsu's emails, telephone calls, and conversations together showed that he believed that the information he sought could not be acquired through legal or public means. Therefore, the court concluded that the EEA's definition of trade secret was not unconstitutionally vague as applied to Hsu. *Id.* at 630-31.

Subsequent courts have upheld the EEA against similar constitutional challenges. *See United States v. Yang*, 281 F.3d 534, 544 n.2 (6th Cir. 2002) (rejecting defendants' argument that the EEA would be unconstitutionally vague if attempt and conspiracy charges need not be based on actual trade secrets, because "[w]e have every confidence that ordinary people seeking to steal information that they believe is a trade secret would understand that their conduct is proscribed by the statute"); *United States v. Kumrei*, 258 F.3d

535, 539 (6th Cir. 2001) (rejecting claim that the "reasonable measures" were unconstitutionally vague); *Chung*, 622 F. Supp. 2d at 974 (concluding "the term 'reasonable measures' is not unconstitutionally vague"); *United States v. Genovese*, 409 F. Supp. 2d 253 (S.D.N.Y. 2005) (denying motion to dismiss indictment as vague by defendant who argued that, having found confidential source code on the Internet, he could not know whether the code was generally known to the public or whether the code's owners took reasonable measures to keep it secret, and ruling that the government's allegations established that the defendant was on notice that the code was proprietary and any protective measures had been circumvented).

D. Preserving Confidentiality and the Use of Protective Orders

One essential objective in any trade secret prosecution is to ensure that an effective protective order is in place to safeguard against disclosure of the trade secret during prosecution of the criminal case. The safeguards should cover each phase of the prosecution, including discovery and any public proceedings, such as a trial or sentencing hearing.

1. Overview

Protective orders, or other appropriate measures, are commonly used in civil cases involving trade secrets. *See, e.g.*, Fed. R. Civ. P. 26(c)(1)(g) (providing for civil protective orders "requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way"); *see also Burlington N.R.R. Co. v. Omaha Pub. Power Dist.*, 888 F.2d 1228, 1232 (8th Cir. 1989) (reviewing contract *in camera* without revealing trade secret); *Canal Refining Co. v. Corrallo*, 616 F. Supp. 1035, 1045 (D.D.C. 1985) (granting plaintiff's motion for protective order to seal separate portions of affidavit designated as exhibit); *see generally* 3 Roger M. Milgrim, Milgrim on Trade Secrets § 14.02[4] (discussing protective orders and other measures). Likewise, protective orders are regularly used in EEA cases to protect against disclosure of trade secrets.

Congress emphasized the need for protective orders in criminal cases involving trade secrets. *See* H. R. Rep. No. 104-788, at 4 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4022 ("The bill requires courts hearing cases brought under the statute to enter such orders as may be necessary to protect

the confidentiality of the information involved in the case."); *id*. at 13, 4032 ("The intent of this section is to preserve the confidential nature of the information and, hence, its value. Without such a provision, owners may be reluctant to cooperate in prosecutions for fear of further exposing their trade secrets to public view, thus further devaluing or even destroying their worth."). The legislative history underscores the importance of courts taking adequate steps to protect trade secrets particularly in the early stages of prosecution even before a determination that the information is a trade secret has been made:

> We have been deeply concerned about the efforts taken by courts to protect the confidentiality of a trade secret. It is important that in the early stages of a prosecution the issue whether material is a trade secret not be litigated. Rather, *courts should, when entering these orders, always assume that the material at issue is in fact a trade secret*.

142 Cong. Rec. 12,213 (Oct. 2, 1996) (Manager's Statement) (emphasis added).

The EEA contains a specific provision authorizing protective orders in trade secret cases. Specifically, § 1835 provides:

> [T]he court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

In addition to § 1835, which applies to EEA cases, prosecutors can alternatively consider Fed. R. Crim. P. 16(d), which provides:

> (1) Protective and Modifying Orders. At any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief. The court may permit a party to show good cause by a written statement that the court will inspect ex parte. If relief is granted, the court must preserve the entire text of the party's statement under seal.

Rule 16(d) has been cited as an alternative legal basis for a protective order in cases involving trade secrets. *See, e.g.*, *United States v. Hsu,* 155 F.3d 189, 193 (3d Cir. 1998) (noting "the government filed a motion pursuant to 18 U.S.C. § 1835 and Fed. R. Crim. P. 16(d)(1) for a protective order to prevent the disclosure of the Bristol–Myers trade secrets allegedly contained in those documents"). Although both provisions authorize protective orders, their coverage and application are distinct. Rule 16(d) applies generally in all criminal cases, whereas § 1835 applies only to cases charging economic espionage, under 18 U.S.C. § 1831, and trade secret misappropriation, under 18 U.S.C. § 1832. Nonetheless, it is common for both legal bases, § 1835 and Rule 16(d), to be cited in an application for a protective order.

In some cases, prosecutors may consider whether to charge the misappropriation of proprietary information as trade secret misappropriation or under other legal theories. *See generally* Section G. of this Chapter (considering other alternative charges). Where trade secrets are involved, however, it is recommended that prosecutors pursue charges under either §§ 1831 or 1832 of the EEA. One benefit from charging violations of the EEA is the ability to use the protections afforded in § 1835 to safeguard trade secrets in the criminal prosecution, such as the ability to seek an interlocutory appeal of a court order to disclose a trade secret, as noted in the next Section.

2. Interlocutory Appeals

Section 1835 expressly allows the government to file "[a]n interlocutory appeal … from a decision or order of a district court authorizing or directing the disclosure of any trade secret." This opportunity for prompt judicial review of a district court decision provides an essential added layer of protection against the disclosure of trade secrets.

Although the language permitting the government to seek interlocutory appeal is broad and without time limits, as a practical matter, the issues concerning court-ordered disclosure of a trade secret should be raised before trial and certainly resolved before jeopardy attaches upon the swearing of the jury.

Since the statute was enacted in 1996, the interlocutory provision has been invoked in two cases, *United States v. Hsu*, 155 F.3d 189 (3rd Cir. 1998), and *United States v. Ye*, 436 F.3d 1117 (9th Cir. 2006). Both times the government prevailed on appeal and averted disclosure of trade secret information, however, for different reasons.

United States v. Hsu (3d Cir. 1998)

The first case to address the use of protective orders under the EEA is *United States v. Hsu*, 155 F.3d 189 (3rd Cir. 1998). *Hsu,* also one of the first cases prosecuted under the statute, presented an early test concerning the disclosure of trade secret information and the new protections provided under § 1835. In *Hsu*, the trade secrets involved processes, methods, and formulas for an anti-cancer drug known as Taxol. One defendant requested and offered to pay for Taxol information, not realizing he was communicating with an undercover agent. After the investigation, three defendants were charged with attempted theft of trade secrets, and a conspiracy to steal trade secrets, along with other charges. The defense moved for a copy of the documents revealed at a key meeting with the undercover agent. The government requested a protective order under § 1835 and Rule 16(d)(1) to prevent disclosure of the trade secrets. The government asked the court to review the materials *in camera* and to redact trade secret information. The government argued that since inchoate crimes of attempt and conspiracy were charged, there was no need to divulge the trade secrets. The defense insisted on receiving unredacted copies. The district court agreed with the defense to adopt an order allowing "select members of the defense team" with access to the documents. The court then "'encourage[d]' the government to file an interlocutory appeal to clarify the 'unsettled and important questions of law' raised by this case." *Hsu*, 155 F.3d at 193-94 (quoting district court opinion). The government filed an interlocutory appeal under § 1835.

On appeal, the Third Circuit reversed the district court ruling after concluding that the incomplete crimes of attempt and conspiracy did not require actual proof of the trade secret. *Hsu*, 155 F.3d at 203-04; *see also* Section B.6. of this Chapter, *supra*. After the case was remanded, the district court concluded the defense was not entitled to receive the unredacted documents. The materials were also unnecessary to support an entrapment or outrageous government conduct defense. *See United States v. Hsu*, 185 F.R.D. 192, 198 & n.19 (E.D. Pa. 1999) (analogizing that it is unnecessary in a drug case involving attempt or conspiracy charges for the defense to have access to the drugs in the case).

Although the *Hsu* case did not involve review of a trade secret case involving actual misappropriation under the substantive provisions of the statute, 18 U.S.C. § 1832(a)(1)-(a)(3), the case demonstrates how the interlocutory appeal

provision was used effectively to advert disclosure of trade secret information pending appellate court review.

United States v. Ye (9th Cir. 2006)

In *United States v. Ye*, 436 F.3d 1117 (9th Cir. 2006), the second case to address interlocutory appeal, decided eight years after *Hsu*, the government sought an interlocutory appeal along with a writ of mandamus. In *Ye*, two defendants were arrested as they tried to board a flight from San Francisco to China. They were found to possess suspected trade secrets from four Silicon Valley companies including technical schematics, information about design methodology, computer aided design scripts, microprocessor specifications, and other technology information. The two defendants were charged with committing economic espionage, the second case charging violations of § 1831, along with trade secret misappropriation and other counts. Before trial, the government provided the defense with "all the trade secret materials" under a protective order, including "more than 8,800 pages of materials, which 'describe the substance of each alleged trade secret.'" *Ye*, 436 F.3d at 1119. The defense requested, and was granted, the opportunity to conduct pre-trial depositions of several government expert witnesses to determine "what exactly is being alleged to be the trade secret and why it is a trade secret in advance of trial." *Id*. After its motion for reconsideration was denied, the government filed an interlocutory appeal under § 1835 and alternatively petitioned for a writ of mandamus under the All Writs Act, 28 U.S.C. § 1651.

The Ninth Circuit concluded that it lacked jurisdiction over the § 1835 interlocutory appeal because "the purpose of the district court's order was only to clarify exactly which materials the government contends constitute the protected trade secrets, and all relevant materials had already been turned over, the district court's order does not direct or authorize the 'disclosure' of trade secrets as required by the plain language of § 1835." *Ye*, 436 F.3d at 1121. In considering the second basis for appellate review, however, the court found that the government established "exceptional circumstances" to warrant a writ of mandamus directing the district court to rescind its ruling. As the court explained:

> After weighing all five [writ of mandamus] factors, we conclude that they lean strongly in favor of granting mandamus relief. The district court's order was 'wholly unauthorized' and 'constitutes a clear and very substantial departure from the fundamental

> principles governing criminal pretrial and trial procedures in federal court.' The government has demonstrated that it has no alternative means of relief and will suffer harm that is not correctable on appeal. Finally, the district court's order raises the new and important question of whether the EEA empowers a court to authorize discovery depositions under Rule 15 in order to ensure fairness and efficiency and effectively control the dissemination of important trade secrets.

Ye, 436 F.3d at 1124 (citations omitted). Consequently, the government prevailed in challenging the district court's discovery order under this alternative, although exceptional, ground.

3. Types of Protective Orders

Generally speaking, three types of protective orders may be appropriate during different stages of a case:

- First, a protective order may be necessary to discuss the case with third parties before charges are filed. Under these circumstances, the protective order, which is typically stipulated to by the parties, should stipulate to jurisdiction in the event any disputes arise.
- Second, after charges are filed, but before any trial, a protective order is essential to ensure that the trade secret is used solely for preparation of the defense and is not divulged to third parties unconnected with the defense.
- Third, a protective order may be required to govern the use of trade secret evidence during a public trial.

Typically, the parties will enter into a stipulation and application for entry of a protective order. Where agreement cannot be reached on selected issues, the court may need to resolve them. It is not uncommon for an interim protective order to be imposed during one stage with the understanding that it may be modified to protect the trade secret and related information at another stage.

Protective orders may also vary depending on the issues in the case. For example, a special protective order may be necessary for a case involving source code. CCIPS has examples of each type of protective order which is available to prosecutors. These model protective orders can be tailored to the facts and issues of the particular case.

As described in the following subsections, although protective orders may vary depending on the trade secrets and issues involved in the case, there are some key and consistent parameters that should be addressed in an application for each type protective order. The protections are different before trial and during trial.

a. Pre-Trial Protective Order Issues

Before trial, protective orders generally govern what information is covered and who may access it without necessarily stipulating that the information is in fact a trade secret. Because the defense may not wish to stipulate that the items are in fact trade secrets, it is not uncommon for the parties to agree that the designated items *may* constitute trade secrets or other confidential or proprietary information, or that the designation merely serves to "to preserve the confidentiality of trade secrets," as required under 18 U.S.C. § 1835. At this stage of the criminal case, the label assigned to the materials is less important than ensuring that they are adequately safeguarded.

The pre-trial protective order will typically restrict access to the defense litigation team solely for defending the case. One important feature of protective orders is that anyone accessing the trade secret materials sign an acknowledgment that they have read and understood the protective order and agree to be bound by its terms, including sanctions for any violations. The signed acknowledgments can be maintained by the government or filed with the court. The protective order usually specifies that:

- the trade secret materials must be maintained in a secure manner and may not leave a designated area;
- if maintained on a computer, the computer may not be connected to the Internet;
- a copy of the protective order shall be kept with the copies of the protected materials at all times;
- any filings of the trade secret materials shall be made filed under seal; and
- the circumstances for the return of the trade secret materials upon the conclusion of the case.

Another pretrial issue that may relate to a trade secret protective order concerns defense use of a subpoena under Fed. R. Crim. P. 17(c) to obtain further information about the trade secrets from the victim company. Prosecutors should consider whether the subpoena seeks information protected

by the protective order, or that has been previously provided. The courts have also recognized that Rule 17(c) cannot be used as a means to obtain general discovery. *See, e.g., United States v. Hardy*, 224 F.3d 752, 756 (8th Cir. 2000) (denying Rule 17(c) subpoena where defendant was attempting to use it as a discovery device, "which it is not"); *United States v. Arditti*, 955 F.2d 331, 345 (5th Cir. 1992) (Rule 17 "is not intended to provide an additional means of discovery"); *see also United States v. Ye*, 436 F.3d 1117, 1124 (9th Cir. 2006) (issuing writ of mandamus to rescind district court order compelling depositions of government expert witnesses concerning trade secrets before trial).

Generally, Rule 17(c) subpoenas should not be issued by the court unless the moving party meets its burden to demonstrate that (1) the documents sought are both evidentiary and relevant, that is, admissible; (2) the documents are not otherwise procurable before trial through reasonable diligence, (3) the party cannot properly prepare for trial without early production; and (4) the application is not intended as a general fishing expedition. *United States v. Nixon*, 418 U.S. 683, 699-700 (1974). CCIPS can provide some sample responses to defense requests for subpoenas under Rule 17(c).

b. Trial Protective Order Issues

Separate issues are involved by the presentation of evidence related to the trade secret at trial. A protective order governing the use of information during trial may apply more specifically to "trade secrets" as defined under 18 U.S.C. § 1839(3), and "trial protected material," which includes trade secret information and related confidential or proprietary information that may reveal or disclose the trade secrets in this case. The scope of this coverage protects against disclosure of not only trade secrets but information related to the trade secret.

The protective order should impose a duty on the parties to notify the court before introducing any protected material at trial. This obligation is important to allow the court and parties to put appropriate and timely measures in place to protect the confidentiality of trade secrets before such material is introduced at trial.

Likewise, prosecutors should consider seeking to include instructions on how trade secret materials may be presented during the trial. For example, the protective order could limit access to exhibit binders exclusively to the jury, the parties, and the court and require the exhibits to be retrieved after the conclusion of the witness testimony. Additionally, the court display or other

monitors shall be similarly confined. *See, e.g.*, *United States v. Roberts*, 2010 WL 1010000, at *9 (E.D. Tenn. Mar. 17, 2010).

Special instructions may be necessary for witnesses and juries as well to protect trade secret material. For example, the parties may instruct witnesses not to disclose the protected materials during the course of their testimony until and unless authorized by the court. Additionally, during the trial and at the conclusion of the case, the jury may be instructed that they are not to disclose or otherwise use the protected material which was presented during the trial. CCIPS has sample trial protective orders for prosecutors.

c. Closing the Courtroom

Where closed proceedings are contemplated, other special requirements apply. First, Department of Justice policy does not permit the closing of the courtroom unless approved by the Deputy Attorney General. See 28 C.F.R. § 50.9; USAM 9-5.150. This presumption against closed proceedings may be overcome upon a showing of certain factors and approval by the Deputy Attorney General. A request for a closed proceeding is initially reviewed through the Office of Enforcement Operations at (202) 305-4023. *Id.*. For a trial example in which the courtroom was closed on a limited number of occasions, see *United States v. Aleynikov*, 2010 WL 5158125, at *1 (S.D.N.Y. Dec. 14, 2010) (noting "Over the course of the eight day trial, the courtroom was closed on seven occasions, most of them lasting no longer than 20 minutes."), *rev'd on other grounds*, 676 F.3d 71 (2d Cir. 2012).

The right to a public criminal trial, under the Sixth and First Amendments, is not absolute and may be limited in certain circumstances. *See Globe Newspaper Co. v. Superior Court for the County of Norfolk*, 457 U.S. 596, 603 (1982) (noting "the press and general public have a constitutional right of access to criminal trials."); *Waller v. Georgia*, 467 U.S. 39, 46 (1984) ("[T]here can be little doubt that the explicit Sixth Amendment right of the accused is no less protective of a public trial than the implicit First Amendment right of the press and public."); *see also Gannett v. DePasquale*, 443 U.S. 368, 419-33 (1979) (Blackmun, J., concurring in part and dissenting in part) (tracing the history of the right to a public trial and citing cases where that right has been limited). Although not absolute, the Supreme Court has held that, "proceedings cannot be closed unless specific, on the record findings are made demonstrating that 'closure is essential to preserve higher values, and is narrowly tailored to serve that interest.'" *Press-Enterprise Co. v. Superior Court of California for*

Riverside, 478 U.S. 1, 13-14 (1986) (citations omitted) (holding there is a First Amendment right of access to the transcript of a preliminary hearing); *Waller,* 467 U.S. at 48 (noting that (i) a "party seeking to close the hearing must advance an overriding interest that is likely to be prejudiced," (ii) "the closure must be no broader than necessary to protect that interest," and (iii) "the trial court must consider reasonable alternatives to closing the proceeding"); *see also In re Copley Press, Inc.*, 518 F.3d 1022, 1028 (9th Cir. 2008) (applying factors, concluding there was "no First Amendment right to access the transcripts of the closed portions of the [plea] hearings on the motions to seal"). Accordingly, if the proceedings are closed, appropriate findings, consistent with this case law, should be made on the record.

4. Return of Trade Secrets Upon Conclusion of the Case

A final step to safeguard trade secrets is to provide for the return of the trade secret material upon the conclusion of the case. The protective order should direct that the defense assemble and return all materials and certify in writing that the required procedures were completed.

To ensure defense counsel is aware of the responsibility to return all trade secret material after a conviction, by trial or plea agreement, the prosecutor should alert the defense and court that the materials will be requested for return shortly after sentencing. One approach used in trade secret cases is to send defense counsel a letter reminding them of the terms under the protective order requiring the return of the trade secret materials upon the conclusion of the case. The letter can request the material be returned at the sentencing hearing or shortly afterwards. The sentencing memorandum can apprise the court of this request which can be renewed at the sentencing hearing. The court can resolve any disagreements under the terms of the protective order.

E. Special Issues

1. Civil Injunctive Relief for the United States

The EEA authorizes the government to file a civil action to "obtain appropriate injunctive relief against any violation of this chapter." *See* 18 U.S.C. § 1836(a). Prosecutors should consider seeking injunctive relief to prevent further disclosure of a trade secret by the defendant or third parties during a criminal investigation, or as part of the judgment at the end of the case.

Prosecutors may even seek injunctive relief in matters that do not warrant criminal prosecution if the victim is unable to do so. Note, however, that most victims can obtain injunctive and monetary relief on their own through state-law statutory and common-law remedies. For an extensive discussion of injunctive relief in civil cases, see 4 Roger M. Milgrim, *Milgrim on Trade Secrets* § 15.02[1].

The civil remedy in § 1836 can be enforced only by the government. Neither that section nor any other section of the EEA creates a private right of action that can be enforced by private citizens. *Cooper Square Realty, Inc. v. Jensen*, No. 04 Civ. 01011 (CSH), 2005 WL 53284 (S.D.N.Y. Jan. 10, 2005); *Barnes v. J.C. Penney Co.*, No. 3-04-CV-577-N, 2004 WL 1944048 (N.D. Tex. Aug. 31, 2004), *magistrate's findings adopted*, 2004 WL 2124062 (N.D. Tex. Sept. 22, 2004).

2. Parallel Proceedings

In light of the significant overlap of elements in civil trade secret misappropriation statutes and the EEA, it is often the case that a prosecutor on an EEA criminal case is confronted with a parallel civil proceeding. A parallel proceeding is simply

> simultaneous or successive investigation or litigation of separate criminal, civil, and administrative actions by different agencies, different branches of government, or private litigants involving a common set of facts.

Office of Legal Education, U.S. Dep't of Justice, *Federal Grand Jury Practice* § 12.1 (2008).

In the context of an EEA prosecution, a parallel proceeding is most likely to arise in the form of a concurrent or pre-existing civil trade secret misappropriation case brought by the victim against one or more of the subjects of the criminal investigation. Additionally, as explained above, § 1836(a) of the statue expressly authorizes the Attorney General to bring a civil action to "obtain appropriate injunctive relief against any violation of this chapter." These parallel civil proceedings will almost certainly generate evidence, in the form of interrogatory responses, deposition or trial testimony, and responses to document requests that would be of interest to a criminal prosecutor and investigator investigating potential criminal violations of the EEA. And in some cases, a victim / civil plaintiff may be more than willing to turn over this

evidence to law enforcement. However, federal prosecutors need to be mindful of both the strategic and ethical implications of parallel proceedings in an EEA prosecution.

Prosecutors looking for more in depth guidance on parallel proceedings across all types of federal criminal prosecutions should consult the *Federal Grand Jury Practice* Manual.

a. Due Process and Prosecutorial Misconduct Considerations

There is nothing inherently wrong, ethically or legally, with parallel proceedings, provided that each proceeding is conducted in good faith. *See, e.g., United States v. Kordel*, 397 U.S. 1 (1970) (approving government's parallel civil and criminal proceedings against defendant); *Abel v. United States*, 362 U.S. 217 (1960) (lacking bad faith, mere cooperation of different branches of the Department of Justice is neither illegitimate or unconstitutional); *Securities & Exchange Comm'n v. Dresser Indus.*, 628 F.2d 1368, 1374 (D.C. Cir. 1980) (*en banc*) ("In the absence of substantial prejudice to the rights of the parties involved, such parallel proceedings are unobjectionable under [United States] jurisprudence."). Misuse of a civil or criminal proceeding for the purpose of benefitting the other proceeding, however, in addition to being improper, may jeopardize the criminal proceeding. Such misuse may include affirmative misstatements of fact or law, conduct involving dishonesty, fraud, deceit, or misrepresentation, or impermissible communications with represented persons.

Professional responsibility questions with regard to a specific factual scenario should be directed to the Department of Justice's Professional Responsibility Advisory Office at (202)514-0458.

As discussed below, three circuits have recently found, on somewhat similar factual records, that parallel civil and criminal proceedings being handled by separate divisions of the U.S. government were not conducted in bad faith, and therefore did not violate due process. The key similarities in those cases were that: (1) there were legitimate bases for the civil actions; (2) the defendants were advised of their Fifth Amendment rights prior to making statements to government questioners in the civil actions; and (3) no misleading statements were made regarding the pendency of any criminal proceedings. *But see United States v. Scrushy*, 366 F. Supp. 2d 1134 (N.D. Ala. 2005) (suppressing testimony given by defendant at deposition in civil action by the Security and Exchange Commission (SEC) where the SEC scheduled the deposition based on the prosecutor's request, and the prosecutor provided topics for the SEC to cover).

In *United States v. Stringer*, 535 F.3d 929 (9th Cir. 2008) the Ninth Circuit considered the conduct of a parallel civil SEC investigation, which led to a criminal referral and prosecution by the U.S. Attorney's Office in Oregon. At the outset of the SEC's investigation, the agency provided a standard letter to the defendants, informing them that it may turn over evidence to criminal investigators. The SEC also advised witnesses of their Fifth Amendment Rights at the beginning of their depositions. The SEC referred the matter for criminal prosecution to the U.S. Attorney's Office early in its case, and provided evidence to the criminal prosecution team during the course of its case. It also scheduled depositions of subjects of the criminal investigation to be held in the jurisdiction of the investigating U.S. Attorney's Office, at the request of the Assistant U.S. Attorney.

The district court granted defendant's motion to dismiss the indictment in which the defendant argued that the government used deceit and trickery to obtain incriminating evidence and statements in the civil proceeding for the criminal proceeding, in violation of Due Process. The Ninth Circuit reversed the district court decision. Central to the Ninth Circuit's ruling were that the SEC made no affirmative misrepresentations and advised defendants of possible criminal referrals at the outset of the civil proceeding. The court further recognized:

> It is significant to our analysis that the SEC began its civil investigation first and brought in the U.S. Attorney later. This tends to negate any likelihood that the government began the civil investigation in bad faith, as, for example, in order to obtain evidence for a criminal prosecution.

Id. at 939.

The Eleventh Circuit reached the same conclusion on similar facts in *United States v. Moses*, 219 Fed. Appx. 847 (11th Cir. 2007), in which a defendant in a criminal securities fraud prosecution argued, unsuccessfully, that the government engaged in prosecutorial misconduct when the SEC deposed him in its civil proceeding shortly before the U.S. Attorney's Office initiated its criminal case. As in *Stringer*, the Eleventh Circuit found that the SEC had a legitimate purpose in pursuing its civil case, and the defendant was advised of his Fifth Amendment rights prior to his deposition. *Id.* at 849-50. In reaching its ruling, the court noted that "[i]t is well established that the federal

government may pursue civil and criminal actions either 'simultaneously or successively.'" *Id*. at 849.

Similarly, in *United States v. Posada Carilles,* 541 F.3d 344 (5th Cir. 2008), the Fifth Circuit Court of Appeals reversed the district court's dismissal of a false statements indictment arising out of the defendant's statements during a naturalization interview. There, the defendant, a high-profile Cuban dissident who had been linked to a terrorist attack decades earlier, had illegally entered the United States and applied for citizenship after he was detained. The immigration officer met with federal prosecutors when preparing for the naturalization interview. At the beginning of the interview, the immigration officer advised the defendant of his Fifth Amendment rights, which the defendant invoked at various times during the interview. Reversing the district court's dismissal of the indictment, the Fifth Circuit held that the immigration officer did not have an affirmative duty to warn the defendant of the possibility of criminal prosecution, provided that she did not make any material misrepresentations. The court concluded: "the mere failure of a government official to warn that an investigation may result in criminal charges does not constitute fraud deceit, or trickery." *Id.* at 355. Also key to the court's ruling were the facts that the defendant, and not the government, initiated the civil proceeding in which he made the false statements while applying for citizenship; the defendant was advised of his Fifth Amendment rights; and the U.S. Citizenship and Immigration Services, like the SEC, is required by law to coordinate with federal law enforcement.

It remains to be seen how a court would address similar types of interaction between prosecutors and private parties who were pursuing a civil trade secret action against the subjects of a criminal investigation. For example, it is uncertain how a court would address a situation where the private litigant met with prosecutors to prepare for depositions of subjects of the criminal investigation, and asked subjects questions proposed by prosecutors. The *Stringer*, *Posada Carilles*, and *Moses* cases suggest that a court would not find a due process violation or prosecutorial misconduct, provided that the civil litigation was for a legitimate, independent purposes, and no material, misleading statements were made regarding the possibility of criminal prosecution.

b. Strategic Considerations

Apart from the ethical considerations outlined above, the potential for parallel proceedings raises other strategic considerations in EEA prosecutions.

While evidence gathered by a trade secret owner in a civil action may assist in developing a criminal case, there is also the potential such evidence may be damaging to a criminal investigation. For example, defendants in civil trade secret proceedings are entitled to liberal discovery, which they use to poke holes in both the secrecy of the alleged trade secret information and in the security measures employed by the victim. Defendants may pursue extensive third-party discovery designed to show that the allegedly secret information is, in fact, known to a variety of entities. Similarly, depositions of employees of the owner of the alleged trade secret information could result in conflicting testimony on what they understand to be secret and not secret. Aggressive discovery could also be employed in an attempt to harass employees of the victim company. In such circumstances, the government may consider bringing a motion to stay the parallel civil proceeding. *See generally Federal Grand Jury Practice*, § 12.9 (discussing motions to stay in detail). Of course, doing so will require making the pending criminal investigation known to its subjects.

3. Significance of Electronic Evidence in Trade Secret and Economic Espionage Act Cases

Electronic evidence has proven particularly significant in recent trade secret and economic espionage cases. Because there are unique challenges in gathering evidence concerning a scheme to misappropriate trade secrets, and some of the evidence may be in a foreign country, electronic evidence may open a window on the unlawful conduct.

a. Examples of Electronic Evidence

Examples of electronic evidence in a trade secret case include:

- email or other communications on the victim company's servers that may demonstrate the misappropriation;
- email or other communications or records obtained during a border search of a laptop either entering or leaving the country;
- records on storage media, such as a thumb drive, or portable hard drive used to transfer or download trade secrets;
- email or other communication records among the targets or co-conspirators planning the misappropriation or discussing venture capital or business formation to use the trade secret;
- cell phone communications and records;
- records obtained after seizing computers or hard drives of targets under investigation.

In addition to supporting trade secret or economic espionage charges, electronic evidence may also illuminate other legal theories that may apply in the case, such as wire or computer fraud.

b. Developing an Electronic Evidence Case Plan

Given the importance of electronic evidence, it is important to develop an Electronic Evidence Case Plan at the inception of the case. As part of the plan, consider what types of electronic evidence may be involved. Also, consider how many places the evidence may be found. For example, an email may be located on the sender and recipient's computer or provider's server.

In such circumstances, investigators and prosecutors should consider issuing a request to preserve electronic evidence pending further legal process. Title 18, United States Code, § 2703(f)(1) provides:

> A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

Under Section 2703(f)(2), the provider must retain the records, pending legal process, "for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity."

For more detailed information on preserving and obtaining electronic evidence see CCIPS's manual on *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*.

c. Case Example: United States v. Meng

The importance of an Electronic Evidence Case Plan was underscored in *United States v. Meng*, No. CR 5:04-20216-JF (N.D. Cal. Aug. 29, 2007), a case involving economic espionage charges under 18 U.S.C. § 1831, trade secret misappropriation under 18 U.S.C. § 1832, violations of the Arms Export Control Act under 22 U.S.C. § 2778, and other related charges. The defendant was suspected of misappropriating trade secrets from a Silicon Valley company and using them in the People's Republic of China. During a three-day visit to attend a conference in the United States, the defendant was arrested based on preliminary evidence found during a border search of the defendant's laptop. Section 2703(f) preservation requests were made for all identified

email accounts shortly after the arrest was made. After an initial indictment was obtained, a search warrant for the known email accounts was issued about thirty days after the arrest and after preservation requests were made.

After receiving the search warrant, one email provider advised that there were about 980 emails in the account. The email provider noted that someone using IP addresses in another country tried to delete approximately 966 emails, during a time after the arrest was made in the case. *See also Meng*, No. CR 04-20216-JF (N.D. Cal. Dec. 13, 2006) at ¶ 37 (Superseding Indictment alleging: "It was further part of the conspiracy that defendant Xiaodong Sheldon Meng, directed, and caused to be directed, another person unknown to the Grand Jury, to delete approximately nine-hundred sixty-six (966) emails from Defendant Xiaodong Sheldon Meng's account at smeng~cn@yahoo.com.cn."). Because a preservation request had been made at the time of the arrest, the later attempt to delete the emails was ineffective and the government was able to obtain all of the contents. Without the preservation request, important evidence used to further the investigation and support the prosecution would not have been available in the case. Ultimately, the defendant pled guilty to violating § 1831 of the Economic Espionage Act and also the Arms Export Control Act. *See United States v. Meng*, No. CR 5:04-20216-JF (N.D. Cal. Aug. 29, 2007).

4. Extraterritoriality

Federal criminal laws are generally presumed not to apply to conduct outside the United States or its territories unless Congress indicates otherwise. *See, e.g., United States v. Corey*, 232 F.3d 1166, 1170 (9th Cir. 2000). Congress made an exception for the EEA. The EEA expressly "applies to conduct outside the United States if—(1) the offender is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or (2) an act in furtherance of the offense was committed in the United States." 18 U.S.C. § 1837.

5. Department of Justice Oversight

Before Congress passed the EEA, the Attorney General promised that all EEA prosecutions under both §§ 1831 and 1832 would be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General of the Criminal Division during the first five years of the from the date the statute was enacted. This requirement was codified at 28 C.F.R. § 0.64-5 and applied to the filing of complaints, indictments, and civil proceedings, but not to search warrant applications or other investigative measures.

After the five-year period elapsed, the approval process was modified. Federal prosecutors may now prosecute 18 U.S.C. § 1832 offenses without prior approval; however, the Attorney General strongly urges consultation with the Computer Crime and Intellectual Property Section (CCIPS) before filing § 1832 charges because of CCIPS's experience in handling these complex cases and its access to valuable information and resources. CCIPS can be reached at (202) 514-1026. CCIPS regularly provides assistance on EEA cases including (1) indictment review; (2) suggestions on proving an intent to benefit a foreign government (a key offense element) under 18 U.S.C. §§ 1831, 1839(1), (2); (3) addressing proof issues in establishing a "trade secret" under 18 U.S.C. §§ 1832, 1839(3); (4) early issue spotting and investigative steps to consider; (5) identifying case strategies and suggesting alternative charging theories; (6) advising on strategies to develop an Electronic Evidence Case Plan to obtain electronic evidence; (7) providing sample pleadings, protective orders, and other documents; and (8) trial and proof issues.

In contrast, the Attorney General renewed the prior approval requirement for initiating prosecutions under 18 U.S.C. § 1831. Approval must be obtained from the Assistant Attorney General for the National Security Division, through the Counterespionage Section. USAM 9-2.400, 9-59.000. The Counterespionage Section can be reached at (202) 233-0986.

F. Penalties

1. Statutory Penalties

a. Imprisonment and Fines

Reflecting the more serious nature of economic espionage sponsored by a foreign government, the maximum sentence for a defendant convicted under 18 U.S.C. § 1831 is 15 years' imprisonment and a fine of $5 million, whereas the maximum sentence for a defendant convicted under 18 U.S.C. § 1832 is 10 years' imprisonment and a fine of $250,000 or twice the monetary gain or loss, or both. *See* 18 U.S.C. §§ 1831(a), 1832(a). Similarly, organizations can be fined up to $10 million for violating § 1831 or $5 million for violating § 1832. 18 U.S.C. §§ 1831(b), 1832(b).

b. Criminal Forfeiture

The EEA provides for both civil and criminal forfeiture. In October 2008, Congress harmonized the criminal forfeiture provisions for all criminal intellectual property violations, including violations of the EEA, in the Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008. The relevant provision is 18 U.S.C. § 2323. Section 1834 of the EEA, which formerly governed criminal forfeiture for violations of the EEA now simply references 18 U.S.C. § 2323.

The following property is subject to both criminal and civil forfeiture in a case brought under the EEA:

> (A) Any article, the making or trafficking of which, is prohibited under ... [the EEA].
>
> (B) Any property used, or intended to be used, in any manner or part to commit or facilitate the commission of [a violation of the EEA].
>
> (C) Any property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of [a violation of the EEA].

18 U.S.C. § 2323(a)(1), (b)(1).

As a procedural matter, the government should allege forfeiture in the indictment. For additional discussion of forfeiture in intellectual property cases, see Chapter VIII of this Manual.

c. Restitution

The PRO-IP Act of 2008 referenced above also harmonized federal criminal law regarding restitution in intellectual property offenses in a single section of the criminal code, 18 U.S.C. § 2323(c). That section now expressly provides that the court shall order a person who has been convicted of an EEA offense, among other criminal intellectual property laws, "to pay restitution to any victim of the offense as an offense against property referred to in 18 U.S.C. § 3663A(c)(1)(A)(ii)."

The Mandatory Victims Restitution Act of 1996 ("MVRA"), codified at 18 U.S.C. § 3663A, requires the court to order restitution in all convictions for, among others, any "offense against property … including any offense

committed by fraud and deceit," and "in which an identifiable victim or victims has suffered a physical injury or pecuniary loss." *See* 18 U.S.C. § 3663A(c)(1)(A)(ii), (B). For cases involving "damage to or loss or destruction of property of a victim of the offense," the MVRA requires that the defendant return the property to its owner. If return of the property is "impossible, impracticable, or inadequate," the MVRA requires the defendant to pay an amount equal to the property's value on the date of its damage, destruction, or loss, or its value at the time of sentencing, whichever is greater, less the value of any part of the property that is returned. *See* 18 U.S.C. § 3663A(b)(1).

As noted, the mandatory restitution statute also applies to any offense where "an identifiable victim or victims has suffered a physical injury or a pecuniary loss." 18 U.S.C. § 3663A(c)(1)(B). Restitution must be ordered "to each victim in the full amount of each victim's losses as determined by the court and without consideration of the economic circumstances of the defendant." 18 U.S.C. § 3664(f)(1)(A). Thus, to the extent a court has already calculated the loss or injury actually suffered by a victim of trade secret theft in determining the offense level under U.S.S.G. § 2B1.1, the same amount could be used for restitution under the MVRA. For additional discussion of restitution in criminal intellectual property cases, see Chapter VIII of this Manual.

2. Sentencing Guidelines

Issues concerning the Sentencing Guidelines are covered in Chapter VIII of this Manual.

G. Other Charges to Consider

When confronted with a case that implicates confidential proprietary information, prosecutors may wish to consider other crimes in addition to or in lieu of EEA charges. Section 1838 of the statute contemplates that other appropriate remedies may be considered, as the statute does not "preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret." Other charges that may be appropriate, depending on the fact of the case, may include:

- **Disclosing government trade secrets, 18 U.S.C. § 1905**, which punishes government employees and contractors who, *inter alia*, "divulge" or "disclose" trade secrets or certain other information to

the extent not authorized by law. *United States v. Wallington*, 889 F.2d 573 (5th Cir. 1989) (affirming defendant's conviction for running background checks on several people whom the defendant's friend suspected of dealing drugs). Defendants face a fine, a year in prison, and removal from office or employment. Congress clarified that Customs and Border Protection (CBP) may disclose to rights-holders information on suspected counterfeit products to determine if the product is prohibited from importation. *See* § 818(g) of the National Defense Authorization Act for FY2012 (NDAA), H.R.1540, Pub. L. No. 112-81, 125 Stat. 1298 (Dec. 31, 2011) (also noting that this provision will expire on the date the Customs Facilitation and Trade Enforcement Reauthorization Act of 2012 is enacted).

- **Unlawfully accessing or attempting to access a protected computer to obtain information**, **18 U.S.C. § 1030(a)(2), (b)**, for access to a computer used for interstate or foreign commerce or by or for a financial institution or the United States government, 18 U.S.C. § 1030(e)(2). The term "information" is to be construed broadly and need not be confidential or secret in nature. S. Rep. No. 104-357, at 7 (1996). "'[O]btaining information' includes merely reading it. There is no requirement that the information be copied or transported." *Id.* A violation is a misdemeanor unless it was committed for commercial advantage or private financial gain, to further any tortious or criminal act, or if the information's value exceeds $5,000. *See* 18 U.S.C. § 1030(c)(2).

  For offenses on or after September 26, 2008, § 1030(a)(2)(C) was amended (1) to remove the requirement that "the conduct involved an interstate or foreign communication" and (2) to broaden the definition of "protected computer" to include those used in or affecting interstate or foreign commerce or communication. *See* Former Vice President Protection Act, Pub. L. No. 110-326, 122 Stat. 3560 (2008).

  Note: There presently is a split in the circuits in construing the terms "exceed[ing] authorized access" to information under the Computer Fraud and Abuse Act. Depending on the facts of the case, CCIPS can provide current guidance on this issue.

- **Unlawfully accessing or attempting to access a protected computer to commit fraud, 18 U.S.C. § 1030(a)(4), (b)**, where the defendant "knowingly and with intent to defraud," accessed or attempted to access

a protected computer without authorization, or in excess of authorized access, and by means of such conduct furthered the intended fraud and obtained anything of value, "unless the object of the fraud and the thing obtained" was computer time worth less than $5,000. What constitutes "fraud" under § 1030(a)(4) is defined broadly. *See* 132 Cong. Rec. 7,189 (1986) ("The acts of 'fraud' that we are addressing in proposed section 1030(a)(4) are essentially thefts in which someone uses a [protected computer] to wrongly obtain something of value from another"); *see also Shurgard Storage Centers, Inc., v. Safeguard Self Storage, Inc*. 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000) (holding that the word "fraud" as used in § 1030(a)(4) simply means "wrongdoing" and does not require proof of the common-law elements of fraud). EEA charges, which generally involve some level of deception and knowing wrongdoing, will often qualify as fraud. Harming a victim's "goodwill and reputation" provides a defendant with something of "value." *See, e.g.*, *In re America Online, Inc.*, 168 F. Supp. 2d 1359, 1380 (S.D. Fla. 2001).

For more information on offenses involving 18 U.S.C. § 1030 generally, see CCIPS's manual *Prosecuting Computer Crimes*.

- **Mail or wire fraud**, **18 U.S.C. §§ 1341, 1343, 1346**, for schemes that use the mail or wires to defraud another of property or confidential and proprietary information. *See, e.g.*, *United States v. Martin*, 228 F.3d 1, 16-19 (1st Cir. 2000) (affirming mail and wire fraud convictions for schemes to obtain confidential business information); *Howley*, 2013 WL 399345, at *5 (affirming wire fraud convictions for taking and emailing photographs containing confidential proprietary information after promising to not take photographs in non-disclosure agreement).

  A scheme to defraud another of property includes intangible property, such as confidential, nonpublic, prepublication, and proprietary information. *Carpenter v. United States*, 484 U.S. 19 (1987) (holding that financial journalist's trading on information gathered for his newspaper column defrauded the newspaper of its right to the exclusive use of the information); *United States v. Wang*, 898 F. Supp. 758, 760 (D. Colo. 1995) (holding that 18 U.S.C. § 1343 applies not just to physical goods, wares, or merchandise, but also to confidential computer files transmitted by wire); *United States v. Seidlitz*, 589 F.2d 152 (4th Cir. 1978) (holding that data the defendant downloaded from

his former employer's computer system qualified as property under the wire fraud statute and a trade secret).

Mail and wire fraud convictions stemming from the theft of trade secrets have been upheld even when charges under the National Transportation of Stolen Property Act (hereinafter "NTSP act") were not applicable based on the facts of the case, 18 U.S.C. §§ 2314-15, *see infra*, were rejected. *See, e.g.*, *Abbott v. United States*, 239 F.2d 310 (5th Cir. 1956) (affirming § 1341 conviction, but finding insufficient evidence to sustain conviction under 18 U.S.C. § 2314 because government failed to prove market value of map or how or who caused the map to be transported). The mail and wire fraud statute's broader scope results from its concern for the theft of "property" generally, as compared to the NTSP Act's focus on the arguably narrower class of "goods, wares and merchandise" used in §§ 2314 and 2315. *See, e.g.*, *Wang*, 898 F. Supp. at 760 (holding that 18 U.S.C. § 1343 applies to items other than physical goods, wares, and merchandise).

Note: In 2010, in a series of cases, *Skilling v. United States*, 130 S. Ct. 2896 (2010); *Black v. United States*, 130 S.Ct. 2963 (2010); and *Weyhrauch v. United States*, 130 S. Ct. 2971 (2010), the Supreme Court held that the honest services fraud statute, 18 U.S.C. § 1346, applies only to bribery and kickback schemes. For a more detailed discussion of 18 U.S.C. §§ 1341 and 1343, refer to USAM 9-43, and contact the Fraud Section of the Criminal Division at (202) 514-7023 for further information and guidance.

- **Criminal copyright infringement**, **17 U.S.C. § 506 and 18 U.S.C. § 2319**, when the defendant stole and reproduced or distributed copyrighted information. The Copyright Act does not preempt trade secret or related charges if the defendant stole confidential copyrighted material. *See Wang*, 898 F. Supp. at 760-61 (holding that Copyright Act did not preempt wire fraud prosecution for stealing confidential copyrighted material); *Association of Am. Med. Colls. v. Princeton Review, Inc.*, 332 F. Supp. 2d 11, 22-24 (D.D.C. 2004) (analyzing issue and collecting cases).
- **Interstate transportation and receipt of stolen property or goods**, the National Transportation of Stolen Property Act (hereinafter "NTSP Act"), which punishes "[w]hoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise,

securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud," 18 U.S.C. § 2314, and "[w]hoever receives, possesses, conceals, stores, barters, sells, or disposes" stolen property that has crossed a state or federal boundary after being stolen, 18 U.S.C. § 2315.

Assuming that particular stolen items qualify as goods, wares, or merchandise, the courts agree that §§ 2314 and 2315 apply when a defendant steals a tangible object — for example, a piece of paper or a computer disk — that contains intellectual property. *See, e.g.*, *United States v. Martin*, 228 F.3d 1, 14-15 (1st Cir. 2000); *United States v. Walter*, 43 M.J. 879, 884 (N.M. Ct. Crim. App. 1996) ("[C]ourts will include intangible property under the [NTSP] act when tied to tangible property and when the intangible property possesses some business value."); *United States v. Brown*, 925 F.2d 1301, 1308 n.14 (10th Cir. 1991) (holding that even though § 2314 does not apply to theft of intangible property through intangible means, § 2314 would apply to the theft of a piece of paper bearing a chemical formula, even if the paper's intrinsic value were insignificant and the item's overall value was almost wholly derived from the intangible intellectual property contained in the chemical formula) (citing *United States v. Stegora*, 849 F.2d 291, 292 (8th Cir. 1988)) (dictum); *United States v. Lyons*, 992 F.2d 1029, 1033 (10th Cir. 1993) (holding that the defendant's theft of "software in conjunction with the theft of tangible hardware distinguishes this case from *Brown*. *Brown* recognizes that the theft of intangible intellectual property in conjunction with the theft of tangible property falls within the ambit of § 2314."); *United States v. Lester*, 282 F.2d 750 (3d Cir. 1960) (holding that originals and copies of geophysical maps made by defendants on the victim's own copying equipment, with the victim's own supplies, are covered under § 2314); *United States v. Seagraves*, 265 F.2d 876 (3d Cir. 1959) (facts similar to *Lester*); *United States v. Greenwald*, 479 F.2d 320 (6th Cir. 1973) (original documents containing trade secrets about fire retardation processes); *cf. Hancock v. Decker*, 379 F.2d 552, 553 (5th Cir. 1967) (holding that state conviction for theft of 59 copies of a computer program was supported by similar federal court rulings under § 2314) (citing *Seagraves*, 265 F.2d at 876).

Courts are divided, however, on whether the NTSP Act applies to a defendant who transfers intangible property through intangible means, such as electronic data transmission or copying from one piece of paper to another. One view is that it does not. In *Brown*, the defendant was charged with transporting (by means unknown) the source code of a computer program from Georgia to New Mexico, but the government could not prove that the defendant had copied the source code onto the victim's diskettes or that he possessed any of the victim's tangible property. *Brown*, 925 F.2d at 1305-09. The Tenth Circuit held that 18 U.S.C. § 2314 did not cover "[p]urely intellectual property," such as the source code appropriated by the defendant: "It can be represented physically, such as through writing on a page, but the underlying, intellectual property itself, remains intangible" and thus "cannot constitute goods, wares, merchandise, securities or moneys which have been stolen, converted or taken within the meaning of §§ 2314 or 2315." *Id.* at 1307-08. In reaching its decision, the court relied on *Dowling v. United States*, 473 U.S. 207 (1985), which held that property that is "stolen" only in the sense that it is copyright infringing does not fall under the NTSP Act. However, the *Brown* court recognized that § 2314 may apply where the item is tangible: "for § 2314 to apply there must be some tangible item taken, however insignificant or valueless it may be, absent the intangible component." *Brown*, 925 F.2d at 1307-08 n.14. The Tenth Circuit has noted this distinction in other cases. *See, e.g., United States v. Lyons*, 992 F.2d 1029, 1033 (10th Cir. 1993) (in a conviction for transporting stolen computer hardware, the value of the stolen computer software could be considered for sentencing notwithstanding *Brown*; "The fact that Mr. Lyons stole the software in conjunction with the theft of tangible hardware distinguishes this case from *Brown*."), *petition for reh'g denied*, 997 F.2d 826 (10th Cir. 1993).

More recently, the Second Circuit reversed a conviction based on the transmission of stolen source code because "the theft and subsequent interstate transmission of purely intangible property is beyond the scope of" § 2314. *United States v. Aleynikov*, 676 F.3d 71, 77 (2d Cir. 2012). *See also* Section F. of Chapter II (discussing application of *Dowling* to charging 18 U.S.C. § 2314 for intellectual property crimes).

Other cases have approved of NTSP Act prosecutions for theft of intangible property including by intangible means. *See, e.g.*, *United*

States v. Alavi, No. CR07–429–PHX–NVW, 2008 WL 1971391 (D. Ariz. May 2, 2008) (denying motion to dismiss § 2314 count based on the claim that computer software is not "goods, wares, merchandise, securities or money"; distinguishing application of *Dowling*); *United States v. Riggs*, 739 F. Supp. 414, 420-21 (N.D. Ill. 1990) (Rejecting defendant's "disingenuous argument that he merely transferred electronic impulses [albeit impulses containing computerized text files belonging to Bell South] across state lines.… This court sees no reason to hold differently simply because [defendant] stored the information inside computers instead of printing it out on paper. In either case, the information is in a transferrable, accessible, even salable form.")

- **Arms Export Control Act, 22 U.S.C. §§ 2778, and the International Traffic in Arms Regulations (ITAR), 22 C.F.R. §§ 120-130**, which prohibits the export or import of U.S. Munitions List items without obtaining a license from the Secretary of State. *See, e.g., United States v. Reyes*, 270 F.3d 1158, 1169 (7th Cir. 2001) ("Conviction on this count required that the government prove beyond a reasonable doubt that Reyes willfully exported or attempted to export an item on the United States Munitions List without having first obtained a license."). "Defense article" includes items or technical data designated on the United States Munitions List, and "technical data recorded or stored in any physical form, models, mockups, or other items that reveal technical data directly relating to items designated [in the Munitions List]." 22 C.F.R. § 120.6. Under USAM 9-90.620 Arms Export Control Act—22 U.S.C. § 2778, "[u]nless the unlicensed shipment has no relevance to the foreign relations of the United States (e.g., smuggling small quantities of weapons), prosecution of violations of the Arms Export Control Act should not be undertaken without prior approval of the National Security Division. In *United States v. Meng*, No. CR 04-20216-JF (N.D. Cal. Aug. 29, 2007) the defendant was convicted under both the Arms Export Control Act and § 1831 of the Economic Espionage Act.
- **False Statement, under 18 U.S.C. § 1001,** may apply where the defendant makes a material false statement to an agent during the investigation. A statement is material under § 1001 if it has a "natural tendency to influence, or [be] capable of influencing, the decision of the decisionmaking body to which it was addressed." *United States v.*

Gaudin, 515 U.S. 506, 509 (1995). *See generally Chung*, 659 F.3d at 830 (in EEA prosecution, finding sufficient evidence at trial to support false statement conviction based on the defendant's false statement that "his boss ... had given him permission to take work documents home").

- **State and local charges.** Many states have laws that specifically address the theft of information. *See, e.g.*, Uniform Trade Secrets Act. If a state lacks a specific trade-secret law, its general theft statutes may apply. Section 1838 of the EEA contains a non-preemption provision which expressly recognizes that other federal and state remedies may apply "for the misappropriation of a trade secret."

V.

Digital Millennium Copyright Act— 17 U.S.C. §§ 1201-1205

A. Introduction

1. DMCA's Background and Purpose

With the advent of digital media and the Internet as a means to distribute such media, large-scale digital copying and distribution of copyrighted material became easy and inexpensive. In response to this development, and to prevent large-scale piracy of digital content over the Internet, in 1997 the World Intellectual Property Organization (WIPO) responded with two treaties, the Copyright Treaty and the Performances and Phonograms Treaty, to prohibit pirates from defeating the digital locks that copyright owners use to protect their digital content from unauthorized access or copying. Specifically, Article 11 of the WIPO Copyright Treaty prescribes that contracting states

> shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restricts acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

See WIPO Copyright Treaty, Apr. 12, 1997, S. Treaty Doc. No. 105-17, art. 11 (1997); WIPO Performances and Phonograms Treaty, Apr. 12, 1997, S. Treaty Doc. No. 105-17, art. 18 (1997) (same with respect to performers or producers of phonograms). The United States signed these treaties on April 12, 1997, and ratified them on October 21, 1998. *See* 144 Cong. Rec. 27,708 (1998) (Resolution of Ratification of Treaties).

To implement these treaties, Congress enacted Title I of the Digital Millennium Copyright Act (DMCA) on October 28, 1998, with the twin

goals of protecting copyrighted works from piracy and promoting electronic commerce. *See* H.R. Rep. No. 105-551 (II), at 23 (1998); S. Rep. No. 105-190, at 8 (1998); *see also Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 440 (2d Cir. 2001); *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1129-30 (N.D. Cal. 2002). Congress accomplished these goals by enacting prohibitions relating to the circumvention of copyright protection systems as set forth in 17 U.S.C. § 1201, and the integrity of copyright management information pursuant to 17 U.S.C. § 1202. *Cf. Microsoft Corp. v. AT&T Corp.*, 550 U.S. 437, 440 (2007) ("Congress is doubtless aware of the ease with which electronic media such as software can be copied, and has not left the matter untouched.") (citing enactment of DMCA).

Criminal enforcement has largely focused on violations of the anti-circumvention and anti-trafficking prohibitions in 17 U.S.C. § 1201, and thus these are the main focus of this chapter. For a more complete discussion of the provisions that protect the integrity of copyright management information, as set forth in 17 U.S.C. § 1202, see Section B.5. of this Chapter.

2. Key Concepts: Access Controls vs. Copy Controls, Circumvention vs. Trafficking

Section 1201 contains three prohibitions. First, it prohibits "circumvent[ing] a technological measure that effectively controls access to a work protected under this [copyright] title." 17 U.S.C. § 1201(a)(1)(A). Second, it prohibits the manufacture of or trafficking in products or technology designed to circumvent a technological measure that controls access to a copyrighted work. 17 U.S.C. § 1201(a)(2). Third, it prohibits the manufacture of or trafficking in products or technology designed to circumvent measures that protect a copyright owner's rights under the Copyright Act. 17 U.S.C. § 1201(b). As noted more fully in Section C. of this Chapter, the DMCA provides several exceptions.

Title I of the DMCA creates a separate private right of action on behalf of "[a]ny person injured by a violation of section 1201 or 1202" in federal district court. 17 U.S.C. § 1203(a). These prohibitions are criminally enforceable against any person who violates them "willfully and for purposes of commercial advantage or private financial gain," excluding nonprofit libraries, archives, educational institutions, and public broadcasting entities as defined by 17 U.S.C. § 118(f). 17 U.S.C. § 1204(a), (b). Although civil actions do not require the claimant to establish that a DMCA violation was "willful" or for

"commercial advantage or private financial gain," the substantive law defining violations of §§ 1201 or 1202 is generally the same for both criminal and civil actions. Thus, published decisions relating to whether a violation of these DMCA sections has occurred in civil cases are instructive in criminal cases.

a. Access Controls vs. Copy/Use Controls

To understand the technical requirements of the DMCA's criminal prohibitions, it is first important to understand what technology the DMCA generally applies to, and what the DMCA outlaws. Congress intended Title I of the DMCA to apply to copyrighted works that are in *digital* format and thus could easily and inexpensively be accessed, reproduced, and distributed over the Internet without the copyright owner's authorization. The DMCA therefore applies to what one might call a "digital lock"—a technological measure that copyright owners use to control who may see, hear, or use copyrighted works stored in digital form. These digital locks are commonly called either "access controls" or "copy controls," depending on what function the digital lock is designed to control.

The DMCA states that a digital lock, or "technological measure" (as the DMCA refers to such locks), constitutes an *access control* "if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3)(B). Thus, as the name suggests, an access control prevents users from accessing a copyrighted work without the author's permission. For example, a technology that permits access to a newspaper article on an Internet website only by those who pay a fee or have a password would be considered an access control. *See* S. Rep. No. 105-190, at 11-12 (1998); *e.g.*, *CoxCom, Inc. v. Chaffee*, 536 F.3d 101, 110 (1st Cir. 2008) (holding that cable company's pay-per-view billing and delivery system that scrambles pay-per-view programming unless subscribers choose to purchase and view it constitutes an access control). In this example, the author (i.e., copyright owner) uses such fees or password requirements as access controls that allow the author to distinguish between those who have the author's permission to read the online article from those who do not. If a user does not pay the fee or enter the password, then the user cannot lawfully read the article or otherwise access it.

The DMCA also prescribes that a digital lock constitutes a *copy control* "if the measure, in the ordinary course of its operation, prevents, restricts, or

otherwise limits the exercise of a right of a copyright owner under this title." 17 U.S.C. § 1201(b)(2)(B). The rights of a copyright owner include the exclusive rights to reproduce the copyrighted work, to prepare derivative works based upon the copyrighted work, to distribute copies by sale or otherwise, to perform the copyrighted work publicly, and to display the copyrighted work publicly. 17 U.S.C. § 106. In other words, such a digital lock prevents someone from making an infringing use of a copyrighted work *after* the user has already accessed the work. *See* S. Rep. No. 105-190, at 11-12 (1998); *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 441 (2d Cir. 2001). Although some courts will refer to such digital locks as "usage controls" because such locks conceivably seek to control all infringing uses, in practice, these digital locks typically control unauthorized copying of the work—hence the name "copy control."

To illustrate an example of a copy control, consider again the online newspaper article referenced above. A technological measure on an Internet website that permits a user to read (i.e., access) the online article but prevents the viewer from making a copy of the article once it is accessed would be a copy control. *See* S. Rep. No. 105-190, at 11-12 (1998). Thus, access and copy controls are different kinds of digital locks that are each designed to perform different functions. Whereas an access control blocks *access* to the copyrighted work—such as a device that permits access to an article on an Internet website only by those who pay a fee or have a password—a copy control protects the copyright itself—such as a device on the same website that prevents the viewer from copying the article once it is accessed.

Although the DMCA's distinction between an "access control" and a "copy control" appears straightforward in principle, courts are not always consistent in how they characterize a particular protection technology. For example, in the 1990s, the DVD industry developed the Content Scramble System (CSS)—an encryption scheme incorporated into DVDs that employs an algorithm configured by a set of "keys" to encrypt a DVD's contents. For a DVD player to display a movie on a DVD encoded with CSS, the DVD player must have the "player keys" and the algorithm from the copyright owner. The Second Circuit characterized this CSS technology as an "access control" because a DVD player with the proper player keys and algorithm from the copyright owner "can display the movie on a television or a computer screen, but does not give a viewer the ability to use the copy function of the computer to copy the movie or to manipulate the digital content." *Corley*, 273 F.3d at 437. More

than one decision out of the Northern District of California, however, viewed the same technology as both an access control and a copy control. *Apple, Inc. v. Psystar Corp.*, 673 F. Supp. 2d 931, 941 (N.D. Cal. 2009), *aff'd in relevant part*, 658 F.3d 1150 (9th Cir. 2011) ("Although Apple's technological measure may have been primarily aimed at controlling access, it also effectively protected its right to copy."); *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1095 (N.D. Cal. 2004). Accordingly, prosecutors should be careful how they characterize technological controls as access or copy controls, and in some instances it may even be advisable for prosecutors to characterize a particular copyright protection system as both.

b. Circumvention vs. Trafficking in Circumvention Tools

Section 1201(a) of the DMCA proscribes two kinds of conduct regarding *access controls*: 1) circumvention of access controls, 17 U.S.C. § 1201(a)(1), and 2) trafficking in technology primarily designed to facilitate circumvention of access controls, 17 U.S.C. § 1201(a)(2). Both of these prohibitions relating to access controls are discussed more fully in Sections B.1. and B.2. of this Chapter.

Unlike § 1201(a), however, Congress did not ban the act of circumventing *copy controls*. Instead, § 1201(b) only prohibits trafficking in technology primarily designed to facilitate the circumvention of copy controls. 17 U.S.C. § 1201(b)(1). Congress expressly chose not to prohibit the circumvention of copy controls in the DMCA because circumventing a copy control is essentially an act of copyright infringement that is already covered by copyright law. S. Rep. No. 105-190, at 12 (1998).

Thus, § 1201(a)(1) (the "anti-circumvention provision") prohibits the actual *use* of circumvention technology to obtain access to a copyrighted work without the copyright owner's authority. "One of Congress' purposes behind enacting the DMCA was targeting the circumvention of technological protections." *MGE UPS Sys., Inc. v. GE Consumer and Indus., Inc.*, 622 F.3d 361, 365 (5th Cir. 2010). In contrast, § 1201(a)(2) and 1201(b)(1) (the "anti-trafficking provisions") focus on the *trafficking* in circumvention technology, regardless of whether such technology ultimately leads a third party to circumvent an access or copy control. *See Davidson & Assocs. v. Jung*, 422 F.3d 630, 640 (8th Cir. 2005); *Corley*, 273 F.3d at 440-41. And with respect to the anti-trafficking provisions, "although both sections prohibit trafficking in a circumvention technology, the focus of § 1201(a)(2) is circumvention of

technologies designed to *prevent access* to a work, and the focus of § 1201(b)(1) is circumvention of technologies designed to *permit access* to a work but *prevent copying* of the work or some other act that infringes a copyright." *Davidson*, 422 F.3d at 640 (emphasis in original); *Ticketmaster L.L.C. v. RMG Techs.*, 507 F. Supp. 2d 1096, 1112 (C.D. Cal. 2007) ("Sections 1201(a)(2) and 1201(b)(1) differ only in that 1201(a)(2), by its terms, makes it wrongful to traffic in devices that circumvent technological measures that *control access to protected works*, while 1201(b)(1) makes it wrongful to traffic in devices that circumvent technological measures that *protect rights of a copyright owner in a work*.") (emphasis in original); *Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1056 (N.D. Cal. 2010) (same).

The following chart illustrates the distinction:

	Access	Copy
Circumventing	§ 1201(a)(1)	No DMCA violation, but potential copyright violation: 17 U.S.C. § 506; 18 U.S.C. § 2319
Trafficking	§ 1201(a)(2)	§ 1201(b)(1)

3. Differences Between the DMCA and Traditional Copyright Law

Whereas copyright law focuses on "direct" infringement of a copyrighted work, the DMCA focuses largely on the facilitation of infringement through circumvention tools and services primarily designed or produced to circumvent an access or copy control. In other words, the DMCA represents a shift in focus from infringement to the tools of infringers.

Before the DMCA was enacted, copyright law had only a limited application to the manufacture or trafficking of tools designed to facilitate copyright infringement. In 1984, the Supreme Court held that "the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses." *Sony v. Universal City Studios*, 464 U.S. 417, 442 (1984). Under this standard, a copy control circumvention tool would not violate copyright law if it were "widely used for legitimate ... purposes" or were merely "capable of substantial noninfringing uses." *Id.*

The DMCA shifts the focus from determining whether the downstream use of equipment will be used for infringement, to determining whether it

was primarily designed to circumvent an access or copy control—even if such equipment were ultimately capable of substantial noninfringing uses. *See* 17 U.S.C. § 1201(a)(2)(A), (b)(1)(A). For example, with respect to software primarily designed to circumvent copy controls on DVDs, courts have held "that legal downstream use of the copyrighted material by customers is not a defense to the software manufacturer's violation of the provisions of § 1201(b)(1)." *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1097-98 (N.D. Cal. 2004); *see also Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 943-44 (N.D. Cal. 2009) ("[T]he fair use of the copyrighted material by end users is not a defense to, and plays no role in determining, liability under the DMCA."). Thus, although trafficking in circumvention technology that is capable of substantial noninfringing uses may not constitute copyright infringement, it may still violate the DMCA if such technology is primarily designed to circumvent access or copy controls. *See RealNetworks, Inc. v. Streambox, Inc.*, No. 2:99CV02070, 2000 WL 127311, at *7 (W.D. Wash. Jan. 18, 2000).

The DMCA also added a new prohibition against circumventing access controls, even if such circumvention does not constitute copyright infringement. 17 U.S.C. § 1201(a)(1)(A). Prior to the DMCA, "the conduct of circumvention [of access controls] was never before made unlawful." S. Rep. No. 105-190, at 12 (1998); *cf. Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178, 1195-96 (Fed. Cir. 2004). By the same token, the DMCA does not contain a parallel prohibition against the use—infringing or otherwise—of copyrighted works once a user has access to the work. *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1121 (N.D. Cal. 2002) (holding that "circumventing use restrictions is not unlawful" under the DMCA); *cf.* S. Rep. No. 105-190, at 12 (1998) ("The copyright law has long forbidden copyright infringements, so no new prohibition was necessary."). The terms "bypass" or "avoid" in the statute do not "encompass use of a copyrighted work subsequent to a circumvention merely because that use would have been subject to a technological measure that would have controlled access to the work, but for that circumvention." *MGE UPS Sys., Inc. v. GE Consumer and Indus., Inc.*, 622 F.3d 361, 366 (5th Cir. 2010).

Although the DMCA "targets the *circumvention* of digital walls guarding copyrighted material (and trafficking in circumvention tools), [it] does not concern itself with the *use* of those materials after circumvention has occurred." *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 443 (2d Cir. 2001); *MGE*

UPS Sys., 622 F.3d at 366 (same); *cf. 321 Studios*, 307 F. Supp. 2d at 1097 (holding that "the downstream uses of the [circumvention] software by the customers of 321 [the manufacturer], whether legal or illegal, are not relevant to determining whether 321 itself is violating [the DMCA]"). At the same time, the DMCA also cautions that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." 17 U.S.C. § 1201(c)(1); *Elcom*, 203 F. Supp. 2d at 1120 ("Congress did *not* ban the act of circumventing the use restrictions ... because it sought to preserve the fair use rights of persons who had lawfully acquired a work"); *MGE UPS Sys.*, 622 F.3d at 366 (applying the DMCA to the "use of a copyrighted work subsequent to a circumvention ... would extend the DMCA beyond its intended purposes to reach extensive conduct already well-regulated by existing copyright laws"); *United States v. Crippen*, No. 09-703, 2010 WL 7198205, at *2 (C.D. Cal. Nov. 23, 2010) ("The plain meaning of § 1201(c) is clear; the law of copyright infringement (and fair use) is not altered by Congress' decision to create liability for the separate act of circumvention in violation of § 1201(a)."). Thus, a criminal defendant who has violated the DMCA by circumventing an access control has not necessarily infringed a copyrighted work under copyright law. Accordingly, prosecutors must apply traditional copyright law instead of the DMCA to prosecute infringing uses of copyrighted works, including the circumvention of copy controls. By the same token, to demonstrate a violation of the DMCA, prosecutors need not establish copyright infringement, nor even an intent to infringe copyrights.

In addition, unlike in a civil copyright claim, a victim's failure to register its copyrighted work is not a bar to a DMCA action. See Section B.1.c. of this Chapter.

4. Other DMCA Sections That Do Not Concern Prosecutors

Of the DMCA's five titles, the only one that need concern prosecutors is Title I, which was codified at 17 U.S.C. §§ 1201-1205. The remaining four titles concern neither criminal prosecutions nor those provisions of the WIPO treaties that the DMCA was originally designed to implement. Title II concerns the liability of Internet service providers for copyright infringement over their networks. It amended the copyright code by enacting a new § 512, which gives Internet service providers some immunity in return for certain business practices, and requires them to obey certain civil subpoenas to identify subscribers alleged to have committed infringement. Section 512 does not, however, authorize criminal subpoenas for the same purpose.

Title III of the DMCA clarifies that a lawful owner or lessee of a computer may authorize an unaffiliated service provider to activate the computer to service its hardware components. Title IV of the DMCA mandates a study of distance learning; permits libraries and archives to use the latest technology to preserve deteriorating manuscripts and other works; and permits transmitting organizations to engage in ephemeral reproductions, even if they need to violate the newly-added anti-circumvention features in the process. Finally, Title V of the DMCA extends the scope of the Copyright Act's protection to boat hulls.

For purposes of this Manual, all references to the DMCA concern Title I unless the context demands otherwise.

B. Elements of the Anti-Circumvention and Anti-Trafficking Provisions

1. Circumventing Access Controls—17 U.S.C. §§ 1201(a)(1) and 1204

The DMCA prohibits "circumvent[ing] a technological measure that effectively controls access to a work protected under this [copyright] title." 17 U.S.C. § 1201(a)(1)(A). To prove a violation of 17 U.S.C. §§ 1201(a)(1) and 1204, the government must establish that the defendant

1. willfully
2. circumvented
3. a technological measure that effectively controls access (i.e., an access control)
4. to a copyrighted work
5. for commercial advantage or private financial gain.

For purposes of the DMCA, prosecutors may look to the law of copyright infringement for guidance regarding the "willfully" element and the "commercial advantage" element. See Chapter II of this Manual.

Two cases from the Federal Circuit have read an additional element into § 1201(a) offenses, holding that the unauthorized access must also infringe or facilitate infringing a right protected by the Copyright Act to establish violations of 17 U.S.C. § 1201(a)(1) and (a)(2). *Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc.* ("*StorageTek*"), 421 F.3d 1307, 1318 (Fed. Cir. 2005) (quoting *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178, 1203 (Fed. Cir. 2004)). Although the results in *Chamberlain* and

StorageTek are consistent with Congress's intent that § 1201(a) apply to measures controlling access to copyrighted works in digital form (see Section B.1.d. of this Chapter), the courts reached those results using a flawed analysis. Neither the DMCA's plain language nor its legislative history permits circumvention of access controls or trafficking in access or copy control circumvention devices to enable a fair use, as opposed to an infringing use.

The Ninth Circuit recently declined to adopt the Federal Circuit's infringement nexus requirement, and explained that the Federal Circuit's approach "is contrary to the plain language of the statute." *MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 950 (9th Cir. 2010), *as amended on denial of reh'g*, (Feb. 17, 2011). The Ninth Circuit further noted "that the legislative history [of the DMCA] supports the conclusion that Congress intended to prohibit even non-infringing circumvention and trafficking in circumventing devices." *Id.*

The government has consistently argued that the DMCA prohibits the manufacture and trafficking in *all* circumvention tools, even those designed to facilitate fair use. See Section C.10.d. of this Chapter. Additionally, unlike the regional circuits, the Federal Circuit does not have the authority to develop a body of case law on copyright law that is independent of the regional circuits. *StorageTek*, 421 F.3d at 1311; *Chamberlain*, 381 F.3d at 1181. Accordingly, until a regional circuit adopts the *StorageTek-Chamberlain* position regarding the additional element to a § 1201(a) offense, prosecutors should oppose any attempts to cite these decisions as meaningful precedent. If a defendant does attempt to rely on these decisions, prosecutors are encouraged to contact CCIPS at (202) 514-1026 for sample briefs and other guidance to oppose them.

a. Circumventing

To "circumvent" an access control "means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A). Thus, to establish this element, the government first must prove that the defendant 1) *bypassed* a technological measure, and 2) did so *without the authority of the copyright owner*.

"Circumvention requires either descrambling, decrypting, avoiding, bypassing, removing, deactivating or impairing a technological measure *qua* technological measure." *I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys.,*

Inc., 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004); *see also Egilman v. Keller & Heckman*, 401 F. Supp. 2d 105, 113 (D.D.C. 2005) (same); *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 443 (2d Cir. 2001). In other words, circumvention of an access control occurs when someone bypasses the technological measure's gatekeeping capacity, thereby precluding the copyright owner from determining which users have permission to access the digital copyrighted work and which do not. *I.M.S.*, 307 F. Supp. 2d at 532. Arguably, "a person circumvents a technological measure only when he *affirmatively* performs an action that disables or voids the measure that was installed to prevent them from accessing the copyrighted material." *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627, 644 (E.D. Pa. 2007) (emphasis added) (holding that law firm did not circumvent robot. txt technological protection measure on Internet Archive website when such measure malfunctioned and allowed access to archived images that otherwise would have been blocked).

For example, in *Corley*, the Second Circuit characterized CSS, the scheme for encrypting digital movies stored on DVDs, as an access control similar to "a lock on a homeowner's door, a combination of a safe, or a security device attached to a store's products." *Corley*, 273 F.3d at 452-53. A licensed DVD player would be, in this metaphor, the homeowner's key to the door. *Id.* The court held that defendant's computer program, called "DeCSS," circumvented CSS because it decrypted the CSS algorithm to enable "anyone to gain access to a DVD movie without using a [licensed] DVD player." *Id.* at 453. DeCSS functions "like a skeleton key that can open a locked door, a combination that can open a safe, or a device that can neutralize a security device attached to a store's products." *Id.* Thus, using DeCSS to play a DVD on an unlicensed player circumvents an access control because it undermines the copyright owner's ability to control who can access the DVD movie. *Id.*

Circumvention does not occur, however, by properly *using* the technological measure's gatekeeping capacity without the copyright owner's permission. *R.C. Olmstead, Inc. v. CU Interface LLC*, 657 F. Supp. 2d 878, 889 (N.D. Ohio 2009) ("Simply put, CUI did not circumvent or bypass any technological measures of the RCO software—it merely used a username and password-the approved methodology—to access the software."); *Egilman*, 401 F. Supp. 2d at 113 (holding that the definition of circumvention is missing "any reference to 'use' of a technological measure without the authority of the copyright owner"); *see also I.M.S.*, 307 F. Supp. 2d at 533 ("Whatever the impropriety of

defendant's conduct, the DMCA and the anti-circumvention provision at issue do not target this sort of activity."). Using CSS as an example, a defendant does not circumvent a DVD's access control, CSS, by merely borrowing another person's licensed DVD player to view the DVD, even if the defendant did not receive permission from the owner of the licensed DVD player to "borrow" the player. No circumvention has occurred because the defendant would not have bypassed CSS. In fact, he would have viewed the DVD exactly as the copyright owner had intended—by using a licensed DVD player. Courts have similarly held that a defendant who without authorization uses a valid password to access a password-protected website containing copyrighted works does not engage in circumvention because the defendant used an authorized password rather than disabled the access control (here, the password protection mechanism). *See Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 692 (D.Md. 2011); *R.C. Olmstead*, 657 F. Supp. 2d at 889; *Egilman*, 401 F. Supp. 2d at 113-14; *I.M.S.*, 307 F. Supp. 2d at 531-33. *But see Actuate Corp. v. Int'l Bus. Machines*, No. C-09-05892, 2010 WL 1340519, at *9 (N.D. Cal. Apr. 5, 2010) ("hold[ing] that unauthorized distribution of passwords and usernames avoids and bypasses a technological measure in violation of sections 1201(a)(2) and (b)(1)"); *Microsoft Corp. v. EEE Bus. Inc.*, 555 F. Supp. 2d 1051, 1059 (N.D. Cal. 2008) ("By distributing a [software license key] without authorization, [defendant] effectively circumvented Microsoft's technological measure to control access to a copyrighted work in violation of [17 U.S.C. § 1201(a)(2)]."). In this example, other charges might be available if the defendant obtained information from a protected computer. *I.M.S.*, 307 F. Supp. 2d at 524-26 (discussing possible violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)).

In addition, for there to be a circumvention pursuant to § 1201(a)(3)(A), the circumvention must occur "without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A). A defendant who decrypts or avoids an access control measure with the copyright owner's authority has not committed a "circumvention" within the meaning of the statute. *See MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 954 n.16 (9th Cir. 2010), *as amended on denial of reh'g*, (Feb. 17, 2011) (adopting the Second Circuit's view in *Corley* that § 1201(a)(3)(A) "plainly exempts from § 1201(a) liability those whom a copyright owner authorizes to circumvent an access control measure").

The fact that a purchaser has the right to use a purchased product does not mean that the copyright owner has authorized the purchaser to circumvent the

product's access controls. For instance, a purchaser of a CSS-encrypted DVD movie clearly has the "authority of the copyright owner" to view the DVD but does not necessarily have the authority to view it on *any* platform capable of decrypting the DVD, *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1096 (N.D. Cal. 2004) (holding "that the purchase of a DVD does not give to the purchaser the authority of the copyright holder to decrypt CSS"), nor "to perform non-licensed functions, such as copying DVD content." *Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 934 (N.D. Cal. 2009); *see also Davidson & Assocs. v. Jung*, 422 F.3d 630, 641 (8th Cir. 2005) (holding that purchasers of interactive gaming software had permission to use the game but lacked the copyright owner's permission to circumvent the encryption measure controlling access to the game's interactive mode). Thus, purchasers of products containing copyrighted works—by virtue of that purchase alone—do not necessarily have the copyright owner's permission to circumvent a technological measure controlling access to the copyrighted work.

b. Technological Measures That Effectively Control Access ("Access Control")

As already noted, 17 U.S.C. § 1201(a) concerns technological measures designed to prevent *access* to a copyrighted work—technology typically referred to as "access controls." A technological measure does not constitute an access control under the DMCA unless it "effectively controls access to a work." 17 U.S.C. § 1201(a)(1)(A). "[A] technological measure 'effectively controls access to a [copyrighted] work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3)(B).

An access control "effectively controls access to a work" if its ordinary function and operation is to control access to a copyrighted work's expression, regardless of whether or not the control is a strong means of protection. *See*, *e.g.*, *321 Studios*, 307 F. Supp. 2d at 1095.

Significantly, courts have rejected the argument that the meaning of the term "effectively" is based on how successful the technological measure is in controlling access to a copyrighted work. *See*, *e.g.*, *id.* (holding that the fact that the CSS decryption keys permitting access to DVDs were "widely available on the internet [sic]" did not affect whether CSS was "effective" under the

DMCA); *Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 932 (N.D. Cal. 2009) (holding that the "allegation that CSS is no longer an effective technological measure because it has already been cracked or hacked, is of no moment"); *Apple, Inc. v. Psystar Corp.*, 673 F. Supp. 2d 931, 941 (N.D. Cal. 2009), *aff'd in relevant part*, 658 F.3d 1150 (9th Cir. 2011) ("'The fact that circumvention devices may be widely available does not mean that a technological measure is not, as the DMCA provides, effectively protecting the rights of copyright owners in the ordinary course of its operation.'") (quoting *Sony Computer Entm't Am., Inc. v. Divineo, Inc.*, 457 F. Supp. 2d 957, 965 (N.D. Cal. 2006)). For example, protection "measures based on encryption or scrambling 'effectively control' access to copyrighted works, although it is well known that what may be encrypted or scrambled often may be decrypted or unscrambled." *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000) (footnote omitted), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

Equating "effectively" with "successfully" "would limit the application of the statute to access control measures that thwart circumvention, but withhold protection for those measures that can be circumvented" and consequently "offer protection where none is needed" while "withhold[ing] protection precisely where protection is essential." *Id.*; *Divineo*, 457 F. Supp. 2d at 965 (same); *321 Studios*, 307 F. Supp. 2d at 1095 (comparing similar argument to the claim that a deadbolt is ineffective because skeleton keys are readily available on the black market); *DVD Copy Control Ass'n*, 641 F. Supp. 2d at 932 (same); *see also MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 954 n.17 (9th Cir. 2010), *as amended on denial of reh'g*, (Feb. 17, 2011) ("The statutory definition of the phrase 'effectively control access to a work' does not require that an access control measure be strong or circumvention-proof. Rather, it requires an access control measure to provide some degree of control over access to a copyrighted work."); *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 549 (6th Cir. 2004) ("[A] precondition for DMCA liability is not the creation of an impervious shield to the copyrighted work .... Otherwise, the DMCA would apply only when it is not needed.") (internal citations omitted).

Although the DMCA does not define "access," at least one court has held that controlling access to a copyrighted work means controlling access to the expression (e.g., controlling the ability to see or to read the actual text of a copyrighted computer program, hear a copyrighted song, or watch a copyrighted movie) contained in a copyrighted work. *Lexmark*, 387 F.3d

at 547 (holding that an authentication sequence that prevented "access" to a copyrighted computer program on a printer cartridge chip by preventing the printer from functioning and the program from executing did not "control[] access" under the DMCA because the copyrighted work's expression (the computer program) was nonetheless "freely readable"); *Auto Inspection Services, Inc. v. Flint Auto Auction, Inc.*, No. 06-15100, 2006 WL 3500868, at *8 (E.D. Mich. Dec. 4, 2006) (holding that a "user detection feature" that "is a part of the program itself and in no way controls access to the source code" does not constitute an access control because "it merely alerts [plaintiff] as to who [sic] is using the Program"). In the context of a computer program, the Sixth Circuit held that an access control under the DMCA must control access to the program's copyrighted expression—i.e., control the ability to see or to read the program's code. *Lexmark*, 387 F.3d at 548.

On the other hand, a technological measure that controls only the function of a copyrighted computer program but leaves the code freely readable is not an access control under the DMCA. *Compare id.* at 547 (holding that there is no precedent deeming a control measure as one that "effectively controls access" under the DMCA "where the [purported] access-control measure left the literal code or text of the computer program or data freely readable") *and MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 952 (9th Cir. 2010), *as amended on denial of reh'g*, (Feb. 17, 2011) (same), *with Agfa Monotype Corp. v. Adobe Sys., Inc.*, 404 F. Supp. 2d 1030, 1036 (N.D. Ill. 2005) (holding that font embedding bits are not technological measures that "effectively control access" because they "have been available for free download from the Internet" and are "not secret or undisclosed. Embedding bits are not encrypted, scrambled or authenticated, and software applications ... need not enter a password or authorization sequence to obtain access to the embedding bits or the specification for the" font) *and Davidson*, 422 F.3d at 641 (holding that a technological measure that controlled access to a computer program's expression that otherwise "was not freely available" "without acts of reverse engineering" constituted an "access control" under the DMCA).

c. To a Copyrighted Work

The access control also must have controlled access to a copyrighted work. *See* 17 U.S.C. § 1201(a)(1)(A), (2)(A)-(C) (referring repeatedly to "a work protected under this title [17]"). The protection of a copyrighted work is an essential element. *See* S. Rep. No. 105-190, at 28-29 (1998). The DMCA's anti-circumvention prohibition does not apply to someone who circumvents access

controls to a work in the public domain, like a book of Shakespeare, because such a protection measure controls access to a work that is not copyrighted. *Cf. United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1131-32 (N.D. Cal. 2002).

A victim's failure to register its copyrighted work is not a bar to a DMCA action. *See I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 531 n.9 (S.D.N.Y. 2004); *Medical Broad. Co. v. Flaiz*, No. Civ.A. 02-8554, 2003 WL 22838094, at *3 (E.D. Pa. Nov. 25, 2003) (finding that "[w]hile a copyright registration is a prerequisite under 17 U.S.C. § 411(a) for an action for [civil] copyright infringement, claims under the DMCA ... are simply not copyright infringement claims and are separate and distinct from the latter") (citation omitted).

d. How Congress Intended the Anti-Circumvention Prohibition to Apply

Courts have acknowledged that, on its face, § 1201(a)(1) prescribes that one unlawfully circumvents an access control even where the ultimate goal of such circumvention is fair use of a copyrighted work. *See*, *e.g., Reimerdes*, 111 F. Supp. 2d at 304 (holding that an unlawful circumvention of a technological measure can occur even though "[t]echnological access control measures have the capacity to prevent fair uses of copyrighted works as well as foul"). Although Congress was concerned that the DMCA's anti-circumvention prohibition could be applied to prevent circumvention of access controls for legitimate fair uses, Congress concluded that strong restrictions on circumvention of access control measures were essential to encourage digital works because otherwise such works could be pirated and distributed over the Internet too easily. *See Lexmark*, 387 F.3d at 549.

For this reason, courts will strictly apply § 1201(a) to copyrighted expression stored in a digital format whereby, for instance, executing encrypted computer code containing the copyrighted expression actually generates the visual and audio manifestation of protected expression. *Lexmark*, 387 F.3d at 548 (holding that Congress intended § 1201(a) to apply where executing "encoded data on CDs translates into music and on DVDs into motion pictures, while the program commands in software for video games or computers translate into some other visual and audio manifestation"); *see also MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 954 (9th Cir. 2010), *as amended on denial of reh'g*, (Feb. 17, 2011) (dynamic non-literal elements of the "World of Warcraft" game protected by the "Warden" program cannot be accessed without connecting to

a "Blizzard" server's log on program); *Nintendo of Am. Inc. v. Chan*, No. CV 09-4203, 2009 WL 2190186, at *3 (C.D. Cal. July 21, 2009) (Nintendo DS security system controls access to Nintendo's copyrighted DS video games by repeatedly transferring information to gain access to the IPL and Boot Code programs); *321 Studios*, 307 F. Supp. 2d at 1095 (movies on DVDs protected by an encryption algorithm (CSS) cannot be watched without a DVD player that contains an access key decrypting CSS); *Davidson*, 422 F.3d at 641 (encrypted algorithm on computer game prevented unauthorized interactive use of computer game online); *Pearl Inv., LLC v. Standard I/O, Inc.*, 257 F. Supp. 2d 326, 349 (D. Me. 2003) ("encrypted, password-protected virtual private network" prevented unauthorized access to copyrighted computer software); *Sony Computer Entm't Am., Inc. v. Gamemasters*, 87 F. Supp. 2d 976, 981 (N.D. Cal. 1999) (game console prevented unauthorized operation of video games); *RealNetworks, Inc. v. Streambox, Inc.*, Civ. No. 2:99CV02070, 2000 WL 127311, at *3 (W.D. Wash. Jan. 18, 2000) (authentication sequence prevented unauthorized access to streaming copyrighted "digital works" online).

On the other hand, Congress did not intend the DMCA to apply (and courts are less likely to apply it) where executing a copyrighted computer program creates no protectable expression (as it would for a work in digital form), but instead results in an output that is purely functional. *See*, *e.g.*, *Lexmark*, 387 F.3d at 548 (holding that a computer chip on a replacement printer cartridge that emulates an authentication sequence executing a copyrighted code on a manufacturer's printer cartridge did not violate § 1201(a) because executing the code merely controls printer functions such as "paper feeding," "paper movement," and "motor control" and therefore "is not a conduit to protectable expression"); *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178, 1204 (Fed. Cir. 2004) (holding that use of a transmitter to emulate a copyrighted computer code in a garage door opener did not violate § 1201(a) because executing the code merely performed the function of opening the garage door).

Accordingly, prosecutors should bear in mind that courts are more inclined to rule that a defendant violated § 1201(a) if his conduct occurred in a context to which Congress intended the statute to apply—i.e., when it involves an access control that protects access to copyrighted expression stored in digital form. For questions on this often technical point, prosecutors may wish to consult CCIPS at (202) 514-1026.

e. Regulatory Exemptions to Liability Under § 1201(a)(1)

Before prosecuting a charge of unlawful access control circumvention, § 1201(a)(1)(A), prosecutors should confirm whether the defendant's actions fall within the Librarian of Congress's latest regulatory exemptions.

Because Congress was concerned that the DMCA's prohibitions against circumventing access controls might affect citizens' noninfringing uses of works in unforeseeable and adverse ways, Congress created a recurring rulemaking proceeding to begin two years after the DMCA's enactment and every three years thereafter. 17 U.S.C. § 1201(a)(1)(C), (D). Thus, the first rulemaking took place in 2000, the second was in 2003, the third was in 2006, and the fourth occurred as an interim rulemaking in 2009 and was promulgated in final form in July of 2010. The fifth DMCA rulemaking proceeding took place in 2012, and concluded in October of 2012. Specifically, the DMCA provides that its prohibition on access circumvention itself, 17 U.S.C. § 1201(a)(1)(A), will not apply to users' control of certain types of works if, upon the recommendation of the Register of Copyrights, the Librarian of Congress concludes that the ability of those users "to make noninfringing uses of [a] particular class of work[]" is "likely to be ... adversely affected" by the prohibition. 17 U.S.C. § 1201(a)(1)(B). The statute makes clear, however, that any exceptions to § 1201(a)(1)(A) adopted by the Librarian of Congress are not defenses to violations of the anti-trafficking provisions contained in § 1201(a)(2) and 1201(b). *See* 17 U.S.C. § 1201(a)(1)(E).

The current exemptions are effective beginning on October 28, 2012, and they are as follows:

- Literary works, distributed electronically, that are protected by technological measures which either prevent the enabling of read-aloud functionality or interfere with screen readers or other applications or assistive technologies when: (i) a copy of such a work is lawfully obtained by a blind or other person with a disability provided that the rights owner is remunerated, as appropriate, for the price of the mainstream copy of the work as made available to the general public through customary channels; or (ii) such work is a nondramatic literary work, lawfully obtained and used by an authorized entity pursuant to 17 U.S.C. 121.
- Computer programs that enable wireless telephone handsets to execute lawfully obtained software applications, where circumvention is

accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the telephone handset.

- Computer programs, in the form of firmware or software, that enable a wireless telephone handset originally acquired from the operator of a wireless telecommunications network or retailer no later than ninety days after the effective date of this exemption to connect to a different wireless telecommunications network, if the operator of the wireless communications network to which the handset is locked has failed to unlock it within a reasonable period of time following a request by the owner of the wireless telephone handset, and when circumvention is initiated by the owner, an individual consumer, who is also the owner of the copy of the computer program in such wireless telephone handset, solely in order to connect to a different wireless telecommunications network, and such access to the network is authorized by the operator of the network.
- Motion pictures on DVDs that are lawfully made and acquired and that are protected by the Content Scrambling System where the person engaging in circumvention believes and has reasonable grounds for believing that circumvention is necessary because reasonably available alternatives, such as noncircumventing methods or using screen capture software as provided for in alternative exemptions, are not able to produce the level of high-quality content required to achieve the desired criticism or comment on such motion pictures, and where circumvention is undertaken solely in order to make use of short portions of the motion pictures for the purpose of criticism or comment in the following instances: (i) noncommercial videos; (ii) documentary films; (iii) nonfiction multimedia ebooks offering film analysis; and (iv) education purposes in film studies or other courses requiring close analysis of film and media excerpts.
- Motion pictures that are lawfully made and acquired via online distribution services and that are protected by various technological protection measures, where the person engaging in circumvention believes and has reasonable grounds for believing that circumvention is necessary because reasonably available alternatives, such as noncircumventing methods or using screen capture software as provided for in alternative exemptions, are not able to produce the level of high-quality content required to achieve the desired criticism or comment

on such motion pictures, and where circumvention is undertaken solely in order to make use of short portions of the motion pictures for the purpose of criticism or comment in the following instances: (i) noncommercial videos; (ii) documentary films; (iii) nonfiction multimedia ebooks offering film analysis; and (iv) educational purposes in film studies or other courses requiring close analysis of film and media excerpts.

- Motion pictures on DVDs that are lawfully made and acquired and that are protected by the Content Scrambling System, where the circumvention, if any, is undertaken using screen capture technology that is reasonably represented and offered to the public as enabling the reproduction of motion picture content after such content has been lawfully decrypted, when such representations have been reasonably relied upon by the user of such technology, when the person engaging in the circumvention believes and has reasonable grounds for believing that the circumvention is necessary to achieve the desired criticism or comment, and where the circumvention is undertaken solely in order to make use of short portions of the motion pictures for the purpose of criticism or comment in the following instances: (i) noncommercial videos; (ii) documentary films; (iii) nonfiction multimedia ebooks offering film analysis; and (iv) educational purposes.
- Motion pictures that are lawfully made and acquired via online distribution services and that are protected by various technological protection measures, where the circumvention, if any, is undertaken using screen capture technology that is reasonably represented and offered to the public as enabling the reproduction of motion picture content after such content has been lawfully decrypted, when such representations have been reasonably relied upon by the user of such technology, when the person engaging in the circumvention believes and has reasonable grounds for believing that the circumvention is necessary to achieve the desired criticism or comment, and where the circumvention is undertaken solely in order to make use of short portions of the motion pictures for the purpose of criticism or comment in the following instances: (i) noncommercial videos; (ii) documentary films; (iii) nonfiction multimedia ebooks offering film analysis; and (iv) educational purposes.

- Motion pictures and other audiovisual works on DVDs that are protected by the Content Scrambling System, or that are distributed by an online service and protected by technological measures that control access to such works, when circumvention is accomplished solely to access the playhead and/or related time code information embedded in copies of such works and solely for the purpose of conducting research and development for the purpose of creating players capable of rendering visual representations of the audible portions of such works and/or audible representations or descriptions of the visual portions of such works to enable an individual who is blind, visually impaired, deaf, or hard of hearing, and who has lawfully obtained a copy of such a work, to perceive the work; provided however, that the resulting player does not require circumvention of technological measures to operate.

See 37 C.F.R. § 201.40 (2012).

2. Trafficking in Access Control Circumvention Tools and Services—17 U.S.C. §§ 1201(a)(2) and 1204

In addition to prohibiting the circumvention of access controls, the DMCA also prohibits the manufacture of, or trafficking in, any technology that circumvents access controls without the copyright owner's permission. 17 U.S.C. § 1201(a)(2). To prove a violation of 17 U.S.C. §§ 1201(a)(2) and 1204, the government must establish that the defendant

1. willfully
2. manufactured or trafficked in
3. a technology, product, service, or part thereof
4. that either:
   a. is primarily designed or produced for the purpose of
   b. "has only limited commercially significant purpose or use other than" or
   c. "is marketed by that person or another acting in concert with that person with that person's knowledge for use in"
5. circumventing an access control without authorization from the copyright owner
6. for commercial advantage or private financial gain.

For purposes of the DMCA, prosecutors may look to the law of copyright infringement for guidance regarding the "willfully" element and the "commercial advantage" element, discussed in Chapter II of this Manual. For

a complete discussion of establishing the element regarding circumventing an access control, see Sections B.1.a.-e. of this Chapter. The Federal Circuit's additional element for establishing a violation of § 1201(a)(2)—that the unauthorized access must also infringe or facilitate infringing a right protected by the Copyright Act—is discussed in Section B.1.

a. Trafficking

Section 1201(a)(2) states that "[n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic in" a technology or service that unlawfully circumvents an access control. To "traffic" in such technology means to engage either in dealings in that technology or service or in conduct that necessarily involves awareness of the nature of the subject of the trafficking. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 325 (S.D.N.Y. 2000), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001). To "provide" technology means to make it available or to furnish it. *Id.* The phrase "or otherwise traffic in" modifies and gives meaning to the words "offer" and "provide." *Id.* Thus, "the anti-trafficking provision of the DMCA is implicated where one presents, holds out or makes a circumvention technology or device available, knowing its nature, for the purpose of allowing others to acquire it." *Id.* This standard for "trafficking," therefore, hinges on evaluating the trafficker's purpose for making the circumvention technology available. *See id.* at 341 n.257 ("In evaluating purpose, courts will look at all relevant circumstances."). Significantly, however, the government need not prove "an intent to cause harm" to establish the trafficking element. *Cf. Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 457 (2d Cir. 2001).

This standard is particularly helpful for determining whether a defendant has trafficked online in unlawful circumvention technology. For example, courts may view a defendant's trafficking to include offering circumvention technology for download over the Internet, or posting links to websites that automatically download such technology when a user is transferred by hyperlink, where the purpose of such linking is to allow others to acquire the circumvention technology. *See*, *e.g.*, *Reimerdes*, 111 F. Supp. 2d at 325, 341 n.257 (holding that offering and providing for download a computer program to circumvent DVD access controls for the purpose of disseminating the program satisfies trafficking element of § 1201(a)(2)). In addition, at least one court has found that posting a hyperlink to web pages "that display nothing more than the [circumventing] code or present the user only with the choice of commencing a download of [the code] and no other content" also constitutes

"trafficking" under the DMCA because the defendant's express purpose in linking to these web pages was to disseminate the circumventing technology. *Id.* at 325.

In contrast, posting a link to a web page that happens to include, among other content, a hyperlink for downloading (or transferring to a page for downloading) a circumvention program would not, alone, constitute "trafficking" in the program "regardless of purpose or the manner in which the link was described." *Id.*; *see also id.* at 341 n.257 ("A site that deep links to a page containing only [the circumventing program] located on a site that contains a broad range of other content, all other things being equal, would more likely be found to have linked for the purpose of disseminating [the program] than if it merely links to the home page of the linked-to site."). This result is consistent with the general principle that a website owner cannot be held responsible for all the content of the sites to which it provides links. *Id.* at 325 n.180 (quotation omitted). Thus, posting a link (or "linking") to a circumvention program could constitute "trafficking" if the person linking to the program 1) knew that the program is on the linked-to site; 2) knew that the program constituted unlawful circumvention technology; and 3) posted the link for the purpose of disseminating that technology. *See id.* at 325, 341.

b. In a Technology, Product, Service, or Part Thereof

Section 1201(a)(2) prohibits trafficking "in any technology, product, service, device, component, or part thereof" that unlawfully circumvents access controls. This language is "all-encompassing: it includes any tool, no matter its form, that is primarily designed or produced to circumvent technological protection." *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1123 (N.D. Cal. 2002). This element is not limited to conventional devices but instead includes "any technology," including computer code and other software, capable of unlawful circumvention. *Reimerdes*, 111 F. Supp. 2d at 317 & n.135. In addition, the government satisfies this element even if only one "part" or feature of the defendant's technology unlawfully circumvents access controls. *See 321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1098 (N.D. Cal. 2004).

c. Purpose or Marketing of Circumvention Technology

Section 1201(a)(2) prohibits trafficking in technology that unlawfully circumvents access controls and either "is primarily designed or produced for th[at] purpose," "has only limited commercially significant purpose or use other

than" such purpose; or is knowingly marketed for such purpose. 17 U.S.C. § 1201(a)(2)(A)-(C). Thus, "only one of the[se] three enumerated conditions must be met" to satisfy this element. *See 321 Studios*, 307 F. Supp. 2d at 1094; *see also Dish Network L.L.C. v. Whitehead*, No. 3:09-cv-532-J-32JRK, 2011 WL 6181732, at *5 (M.D. Fla. Dec. 13, 2011); *EchoStar Satellite LLC v. ViewTech, Inc.*, Case No. 07cv1273, 2011 WL 1522409, at *2 (S.D. Cal. April 20, 2011). And, as noted elsewhere, the fact that a particular circumvention technology is capable of substantial noninfringing uses is not a defense to trafficking in technology that circumvents access controls and violates one of the three conditions enumerated in § 1201(a)(2)(A)-(C). *See Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 941 (N.D. Cal. 2009) ("no grounding in law ... to assert a 'fair use' defense based on [circumvention technology] being capable of substantial noninfringing use"); *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 323-24 (S.D.N.Y. 2000), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001); *RealNetworks, Inc. v. Streambox, Inc.*, No. 2:99CV02070, 2000 WL 127311, at *8 (W.D. Wash. Jan. 18, 2000).

i. Primarily Designed or Produced

Trafficking in circumvention technology violates § 1201(a)(2)(A) where its "primary purpose" is to circumvent technological measures controlling access to, for example, copyrighted video games (*Davidson & Assocs. v. Jung*, 422 F.3d 630, 641 (8th Cir. 2005); *Sony Computer Entm't Am., Inc. v. Gamemasters*, 87 F. Supp. 2d 976, 987 (N.D. Cal. 1999)); copyrighted streaming video or music content (*Streambox*, No. 2:99CV02070, 2000 WL 127311, at *7-*8); copyrighted satellite programming (*Dish Network, L.L.C. v. SatFTA*, No. 5:08-cv-01561, 2011 WL 856268, at *3-*4 (N.D. Cal. 2011 March 9, 2011)); and copyrighted movies encrypted onto DVDs (*Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 318-19 (S.D.N.Y. 2000), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001); *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1098 (N.D. Cal. 2004); *Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 933 (N.D. Cal. 2009)).

Whether a technology's "primary purpose" is to circumvent an access control is determined by the circumvention technology's primary function, not the trafficker's subjective purpose. *DVD Copy Control Ass'n*, 641 F. Supp. 2d at 940 ("it is the product's function and not the designer's motivation that determines liability"); *see also Reimerdes*, 111 F. Supp. 2d at 319 (motivation

of developer "immaterial" to whether the defendants "violated the anti-trafficking provision of the DMCA"). The defendant's subjective motive may, however, affect whether his conduct falls within one of the DMCA's statutory exceptions. *Id.* (Conduct at issue "prohibited [under DMCA] irrespective of why the [circumvention technology] was written, except to whatever extent motive may be germane to determining whether [defendants'] conduct falls within one of the statutory exceptions."). See Section C. of this Chapter for an overview of these exceptions.

In *Reimerdes*, which concerned the CSS DVD-encryption scheme, the court found that "(1) CSS is a technological means that effectively controls access to plaintiffs' copyrighted works, (2) the one and only function of [the defendant's program] is to circumvent CSS, and (3) defendants offered and provided [the program] by posting it on their web site." *Reimerdes*, 111 F. Supp. 2d at 319. The court held that it was "perfectly obvious" that the program "was designed primarily to circumvent CSS." *Id.* at 318. Defendants argued that their program was not created for the "purpose" of pirating copyrighted movies, but rather to allow purchasers of DVDs to play them on unlicensed DVD players running the Linux operating system. *Id.* at 319. As the court held, however, "whether the development of a Linux DVD player motivated those who wrote [the program] is immaterial to the question" of whether the defendants "violated the anti-trafficking provision[s] of the DMCA." *Id.*; *see also DVD Copy Control Ass'n*, 641 F. Supp. 2d at 940. The trafficking "of the program is the prohibited conduct—and it is prohibited irrespective of why the program was written." *Reimerdes*, 111 F. Supp. 2d at 319. And it is equally irrelevant for whom the program was written. *See Sony Computer Entm't Am., Inc. v. Divineo, Inc.*, 457 F. Supp. 2d 957, 965 (N.D. Cal. 2006) ("The fact that users of mod chips must be technologically sophisticated is not evidence that the purpose of the mod chips is not circumvention.").

ii. Limited Commercially Significant Purpose Other Than Circumvention

Whether a technology has only limited commercially significant purpose other than circumvention is a separate inquiry from whether its primary purpose was to circumvent, and it requires a fact-specific inquiry that often hinges on whether the circumvention technology is "free and available." Some courts, however, have ruled that a particular technology "is primarily designed or produced for the purpose of circumventing" access controls (§ 1201(a)(2)(A)) and also "has only limited commercially significant purpose" other than such

circumvention (§ 1201(a)(2)(B)). *See*, *e.g.*, *Davidson*, 422 F. 3d at 641 (holding that defendant's circumvention technology "had limited commercial purpose because its sole purpose was ... circumventing [the] technological measures controlling access to Battle.net and the [computer] games"); *Streambox*, No. 2:99CV02070, 2000 WL 127311, at *8 (holding that defendant violated § 1201(a)(2)(A) and (a)(2)(B) by trafficking in circumvention technology that had "no significant commercial purpose other than to enable users to access and record protected content"). However, at least one court suggested that whether a defendant violates § 1201(a)(2)(B) "is a question of fact for a jury to decide," even where the court otherwise finds that the defendant has violated § 1201(a)(2)(A). *321 Studios*, 307 F. Supp. 2d at 1098.

iii. Knowingly Marketed for Circumvention

When accused of having marketed technology for use in circumventing access controls in violation of § 1201(a)(2)(C), defendants have raised First Amendment defenses—particularly where only a part of a product circumvents access controls—contending that marketing the product may include dissemination of information about the product's other, legal attributes. Although a more complete discussion analyzing the DMCA's validity under the First Amendment is discussed in Section C.10.b. of this Chapter, it is worth noting here that "the First Amendment does not protect commercial speech that involves illegal activity," even if that commercial speech is merely instructions for violating the law. *321 Studios*, 307 F. Supp. 2d at 1098-99 (citing *Florida Bar v. Went For It, Inc.*, 515 U.S. 618, 623-24 (1995)); *see also Corley*, 273 F.3d at 447 (citing *United States v. Raymond*, 228 F.3d 804, 815 (7th Cir. 2000) (holding that "First Amendment does not protect instructions for violating the tax laws")). Thus, knowingly marketing technology for use in circumventing access controls in violation of § 1201(a)(2)(C) constitutes illegal activity, and hence, unprotected speech. *321 Studios*, 307 F. Supp. 2d at 1099 ("[A]s 321 markets its software for use in circumventing CSS, this Court finds that 321's DVD copying software is in violation of the marketing provisions of §§ 1201(a)(2) and (b)(1).").

3. Trafficking in Tools, Devices, and Services to Circumvent Copy Controls—17 U.S.C. §§ 1201(b)(1) and 1204

As noted above, the DMCA prohibits the manufacture or trafficking in any technology that circumvents copy controls without the copyright owner's

permission. 17 U.S.C. § 1201(b)(1). To prove a violation of 17 U.S.C. §§ 1201(b)(1) and 1204, the government must establish that the defendant

1. willfully
2. manufactured or trafficked in
3. a technology, product, service, or part thereof
4. that either:
   a. "is primarily designed or produced for the purpose of"
   b. "has only limited commercially significant purpose or use other than" or
   c. "is marketed by that person or another acting in concert with that person with that person's knowledge for use in"
5. "circumventing"
6. "protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof"
7. "for commercial advantage or private financial gain."

See 17 U.S.C. §§ 1201(a)(2)(A)-(C), 1204. For purposes of the DMCA, prosecutors may look to the law of copyright infringement for guidance regarding the "willfully" element and the "commercial advantage" element. See Chapter II of this Manual. In addition, because the second, third, and fourth elements of a § 1201(b) violation operate in the same way as do the comparable elements of a § 1201(a) violation, a complete discussion of those elements may be found in Sections B.1. and B.2. of this Chapter.

a. Circumventing

To "circumvent protection afforded by a technological measure," as set forth in 17 U.S.C. § 1201(b), "means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure." 17 U.S.C. § 1201(b)(2)(A). To establish this element, the government must show that the defendant trafficked in technology allowing the end user to bypass a copy or use control that "effectively protects the right of a copyright owner." 17 U.S.C. § 1201(b)(1), (b)(2)(B). Courts have found that the following technologies circumvent copy controls: (1) a computer program that removes user restrictions from an "ebook" to make such files "readily copyable" and "easily distributed electronically," *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1118-19 (N.D. Cal. 2002); (2) technology that bypasses copy controls intended to prevent the copying of streaming copyrighted content, *RealNetworks, Inc. v.*

Streambox, Inc., No. 2:99CV02070, 2000 WL 127311, at *6-*8 (W.D. Wash. Jan. 18, 2000); (3) technology that bypasses copy controls intended to prevent the copying of copyrighted Nintendo DS video games, *Nintendo of Am. Inc. v. Chan*, No. CV 09-4203, 2009 WL 2190186, at *3 (C.D. Cal. July 21, 2009); and (4) technology that bypasses a scheme intended to "control copying of [encrypted] DVDs," *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1097 (N.D. Cal. 2004). Further, at least two courts have held that bypassing a DVD's access and copy controls unlawfully "avoids and bypasses" (i.e., circumvents) the DVD's copy control pursuant to § 1201(b)(2)(A). *Id.* at 1098; *Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 935 (N.D. Cal. 2009).

b. Technological Measure That Effectively Protects a Right of a Copyright Owner Under This Title ("Copy Control")

"[A] technological measure 'effectively protects a right of a copyright owner under this title' if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title." 17 U.S.C. § 1201(b)(2)(B). The "rights of a copyright owner" include all the exclusive rights set forth in 17 U.S.C. § 106: the rights to reproduce the copyrighted work, to prepare derivative works based upon the copyrighted work, to distribute copies by sale or otherwise, to perform the copyrighted work publicly, and to display the copyrighted work publicly. *Elcom*, 203 F. Supp. 2d at 1124. Thus, a technological measure "'effectively protects the right of a copyright owner' if, in the ordinary course of its operation, it prevents, restricts or otherwise limits the exercise of any of the rights set forth in Section 106." *See id.* at 1124 (quoting 17 U.S.C. § 1201(b)(2)(B)); *Agfa Monotype Corp. v. Adobe Sys., Inc.*, 404 F. Supp. 2d 1030, 1039 (N.D. Ill. 2005) (holding that computer font embedding bits do not protect the rights of a copyright owner where "[s]uch embedding bits do not prevent copying, and a computer program can simply proceed to copy the ... [f]ont data regardless of the setting of the bit").

Notably, the government has successfully taken the position that although fair use normally limits a copyright owner's right to claim infringement, § 1201(b)(1) nonetheless prohibits trafficking in *all* tools that circumvent copy controls, even if such tools circumvent copy protections for the purpose of facilitating fair uses of a copyrighted work. *See*, *e.g.*, *Elcom*, 203 F. Supp. 2d at 1124 ("Nothing within the express language would permit trafficking in devices designed to bypass use restrictions in order to enable a fair use, as opposed

to an infringing use."). Hence, § 1201(b)(1) bans trafficking in all tools that are primarily designed or produced for the purpose of circumventing copy controls, regardless of whether the downstream use of such tools is infringing or not. *See id*. "It is the technology itself at issue, not the uses to which the copyrighted material may be put." *321 Studios*, 307 F. Supp. 2d at 1097; *accord Dish Network, L.L.C. v. SatFTA*, No. 5:08-cv-01561, 2011 WL 856268, at *4 (N.D. Cal. March 9, 2011) (holding defendant liable for § 1201(b)(1) violations and explaining that "[w]hile the DMCA provides for a limited 'fair use' exception for certain end users of copyrighted works, the exception does not apply to manufacturers or traffickers ...") (quoting *Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 942 (N.D. Cal. 2009); *Sony Computer Entm't Am., Inc. v. Divineo, Inc.*, 457 F. Supp. 2d 957, 965 (N.D. Cal. 2006) ("downstream customers' lawful or fair use of circumvention devices does not relieve [defendant] from liability for trafficking in such devices under the DMCA"). This is consistent with Congress's intent in enacting the DMCA: "Congress did not ban the act of circumventing the use restrictions. Instead, Congress banned only the trafficking in and marketing of devices primarily designed to circumvent the use restriction protective technologies. Congress did not prohibit the act of circumvention because it sought to preserve the fair use rights of persons who had lawfully acquired a work." *Elcom*, 203 F. Supp. 2d at 1120 (emphasis omitted); *Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 942 (N.D. Cal. 2009) (same); *see also Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 443 (2d Cir. 2001) ("[T]he DMCA targets the circumvention of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the use of those materials after circumvention has occurred.") (emphasis and citations omitted).

Accordingly, while it is not unlawful to *circumvent* a copy or usage control for the purpose of engaging in fair use, it is unlawful under § 1201(b)(1) to *traffic* in tools that allow fair use circumvention. *Elcom*, 203 F. Supp. 2d at 1125; *DVD Copy Control Ass'n*, 641 F. Supp. 2d at 942 (same). Further, "legal downstream use of the copyrighted material by customers is not a defense to the software manufacturer's violation of the provisions of § 1201(b)(1)." *321 Studios*, 307 F. Supp. 2d at 1097-98.

4. Alternate § 1201(b) Action—Trafficking in Certain Analog Videocassette Recorders and Camcorders

Congress's decision to include a prohibition regarding analog technology may be a *non sequitur* in an act entitled the "Digital Millennium Copyright Act." Nonetheless, § 1201(k)(5) of the DMCA prescribes that any violation of 17 U.S.C. § 1201(k)(1) regarding copy controls on certain analog recording devices "shall be treated as a violation of" § 1201(b)(1). Section 1201(k)(1)(A) proscribes trafficking in any VHS, Beta, or 8mm format analog video cassette recorder or 8mm analog video cassette camcorder unless such recorder or camcorder "conforms to the automatic gain control copy control technology." 17 U.S.C. § 1201(k)(1)(A)(i)-(iv). The same prohibition applies to any "analog video cassette recorder that records using an NTSC format video input." 17 U.S.C. § 1201(k)(1)(A)(v). Section 1201(k)(1)(B) also prohibits trafficking in any VHS or 8mm format analog video cassette recorder if the recorder's design (previously conforming with § 1201(k)(1)(A)) was modified to no longer conform with automatic gain control copy technology. 17 U.S.C. § 1201(k)(1)(B)(i). Similarly, the DMCA prohibits trafficking in such an analog video cassette recorder if it "previously conformed to the four-line colorstripe copy control technology" but was later modified so that it "no longer conforms to such technology." 17 U.S.C. § 1201(k)(1)(B)(ii). In addition, the DMCA requires "manufacturers that have not previously manufactured or sold VHS [or 8mm] format analog video cassette recorder[s] to conform to the four-line colorstripe copy control technology." *Id.*

Notably, § 1201(k) does not (1) require analog camcorders to conform to the automatic gain control copy control technology for video signals received through a camera lens; (2) apply to the manufacture or trafficking in any "professional analog video cassette recorder;" or (3) apply to transactions involving "any previously owned analog video cassette recorder" that had been both legally manufactured and sold when new and also not later modified to violate § 1201(k). 17 U.S.C. § 1201(k)(3)(A)-(C).

5. Falsifying, Altering, or Removing Copyright Management Information—17 U.S.C. § 1202

Section 1202 prohibits anyone from knowingly falsifying, removing, or altering "copyright management information"—such as a copyrighted work's title, copyright notice, or author—with the intent to induce, enable, facilitate, or conceal infringement. 17 U.S.C. § 1202(a)(1), (b)(1), (c) (defining

"copyright management information"). Section 1202 further prohibits intentionally facilitating infringement by knowingly distributing or importing for distribution (1) false copyright management information or (2) copyright management information knowing that such information has been removed or altered without authority. 17 U.S.C. § 1202(a)(2), (b)(2). Finally, § 1202 prohibits anyone from intentionally facilitating infringement by distributing, importing for distribution, or publicly performing copyrighted works, copies of works, or phonorecords knowing that their copyright management information has been removed or altered without authority. 17 U.S.C. § 1202(b)(3).

Thus, while § 1201 primarily targets circumvention devices and technology, "Section 1202 imposes liability for specified acts. It does not address the question of liability for persons who manufacture devices or provide services." H.R. Rep. No. 105-551 (I), at 22 (1998). Like § 1201, however, to establish a criminal violation of § 1202, the government must prove two elements in addition to those in the statute itself—that the defendant violated § 1202 both (1) willfully and (2) for purposes of commercial advantage or private gain. 17 U.S.C. § 1204(a). Criminal enforcement of § 1202 of the DMCA is rare, and prosecutors are encouraged to contact CCIPS at (202) 514-1026 for guidance when considering a charge under this provision.

C. Defenses

The DMCA provides for several statutory defenses, exceptions, and even "exemptions" to the anti-circumventing and anti-trafficking prohibitions set forth in 17 U.S.C. § 1201. As the following discussion demonstrates, these defenses do not apply uniformly to the anti-circumvention (§ 1201(a)(1)(A)) and anti-trafficking provisions (§ 1201(a)(2), (b)).

1. Statute of Limitations

Section 1204(c) of the DMCA states that "[n]o criminal proceeding shall be brought under this section unless such proceeding is commenced within 5 years after the cause of action arose." 17 U.S.C. § 1204(c).

2. Librarian of Congress Regulations

The Librarian of Congress promulgates regulatory exemptions every three years that apply only to § 1201(a)(1)(A)'s prohibitions against circumventing access controls. See Section B.1.e. of this Chapter.

3. Certain Nonprofit Entities

Section 1204(b) exempts from criminal prosecution all nonprofit libraries, archives, educational institutions, or public broadcasting entities as defined by 17 U.S.C. § 118(f). *See also* 17 U.S.C. § 1201(d) (listing other entities). The exception set forth in § 1201(d) for nonprofit libraries, archives, and educational institutions is not as broad as the exemption from criminal prosecution for the same group of entities set forth in § 1204(b), because the latter (1) also includes "public broadcasting entities" and (2) precludes prosecution for the anti-circumvention and the anti-trafficking violations of § 1201.

4. Information Security Exemption

"[A]ny lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee" or contractor of the federal government or a state government is exempt from all three of § 1201's prohibitions for information security work on "a government computer, computer system, or computer network." 17 U.S.C. § 1201(e). Congress intended that the term "computer system" would have the same meaning in § 1201(e) as it does in the Computer Security Act. H.R. Conf. Rep. No. 105-796, at 66 (1998), *reprinted in* 1998 U.S.C.C.A.N. 639, 643.

This exemption is narrower than it might first appear. Congress intended this exemption to permit law enforcement to lawfully disable technological protection measures protecting copyrighted works (e.g., measures protecting access to copyrighted computer software) to probe internal government computer systems to ensure that they are not vulnerable to hacking. *Id.* at 65-66. Thus, "information security" consists of "activities carried out in order to identify and address the vulnerabilities of a *government* computer, computer system, or computer network." 17 U.S.C. § 1201(e) (emphasis added); *see also* H.R. Conf. Rep. No. 105-796, at 8.

5. Reverse Engineering and Interoperability of Computer Programs

Section 1201(f) contains three reverse engineering or "interoperability" defenses for individuals using circumvention technology "'for the sole purpose' of trying to achieve 'interoperability' of computer programs through reverse engineering." *Davidson & Assocs. v. Jung*, 422 F.3d 630, 641-42 (8th Cir. 2005) (quoting 17 U.S.C. §1201(f)). Note that at least one court has held that reverse engineering can satisfy the statutory fair use exception. *Bowers v. Baystate Techs., Inc.*, 320 F.3d 1317, 1325 (Fed. Cir. 2003).

The key term for these defenses, "interoperability," "means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged." 17 U.S.C. § 1201(f)(4). The scope of these exemptions is expressly limited to "computer programs" and does not authorize circumvention of access controls that protect other classes of copyrighted works, such as movies. *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, 218 (S.D.N.Y. 2000).

The first interoperability defense allows a person "who has lawfully obtained the right to use a copy of a computer program ... for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to th[at] person" to circumvent an access control without violating the DMCA's anti-circumvention prohibition set forth in § 1201(a)(1)(A). 17 U.S.C. § 1201(f)(1). By definition, this exemption does not apply to one who obtains a copy of the computer program illegally.

Second, § 1201(f)(2) exempts violations of the DMCA's anti-trafficking provisions (§ 1201(a)(2), (b)) for those who "develop and employ technological means" that are "necessary" to enable interoperability. Despite the statute's express requirement that this defense only applies "if such means are necessary to achieve such interoperability," 17 U.S.C. § 1201(f)(2), at least one court has held that "the statute is silent about the degree to which the 'technological means' must be necessary, if indeed they must be necessary at all, for interoperability." *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 551 (6th Cir. 2004).

Third, § 1201(f)(3) authorizes one who acquires information through § 1201(f)(1) to make this information and the technical means permitted under § 1201(f)(2) available to others "solely for the purpose of enabling interoperability of an independently created computer program with other programs." 17 U.S.C. § 1201(f)(3). Significantly, § 1201(f)(3) "permits information acquired through reverse engineering to be made available to others *only by the person who acquired the information*." *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 320 (S.D.N.Y. 2000), *aff'd sub nom., Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001) (emphasis added). Consequently, one court disallowed this defense because, *inter alia*, the defendants "did not do any reverse engineering [themselves]. They simply took [the program] off someone else's web site and posted it on their own." *Id.*

None of these defenses apply if the defendant's conduct also constituted copyright infringement or, in the case of the third defense, otherwise "violate[d] applicable law." *See* 17 U.S.C. § 1201(f)(1)-(3); *see also Lexmark*, 387 F.3d at 551 (holding that defendant, which produced a computer chip that allowed a remanufactured printer cartridge to interoperate with another's originally manufactured printer, did not commit infringement because the computer program that defendant had copied from plaintiff was not copyrighted).

To establish a violation of the anti-trafficking provisions, prosecutors need not establish that the defendant's motive for manufacturing or trafficking in a circumvention tool was to infringe or to permit or encourage others to infringe. *See Reimerdes*, 111 F. Supp. 2d at 319. In contrast, to determine whether defendants meet the interoperability exemption, prosecutors must determine whether the defendant's motive for developing or trafficking the technological means for circumventing an access or copy control was "solely for the purpose" of achieving or enabling interoperability. *Id.* at 320.

Courts strictly apply the requirement that circumvention and dissemination occur "solely for the purpose" of achieving interoperability and not to facilitate copyright infringement. For example, one court has held that circumventing a copyrighted computer game's access controls for the purpose of developing and disseminating a copy or "emulator" that was essentially identical to the original but lacked the original's access control, "constituted more than enabling interoperability" under § 1201(f)(1) and "extended into the realm of copyright infringement." *Davidson & Assocs., Inc. v. Internet Gateway, Inc.*, 334 F. Supp. 2d 1164, 1185-87 (E.D. Mo. 2004) ("The defendants' purpose in developing the bnetd server was to avoid the anti-circumvention restrictions of the game and to avoid the restricted access to Battle.net. Thus, the sole purpose of the [] emulator was not to enable interoperability."), *aff'd*, 422 F.3d at 642 ("Appellant's circumvention in this case constitutes infringement."); *cf. Reimerdes*, 111 F. Supp. 2d at 320 (holding that the purpose of [the defendant's program] was simply to decrypt DVD access controls and not, as defendants claimed, to achieve interoperability between computers running Linux operating system because [the program] also could be used to decrypt and play DVDs on unlicensed players running the Windows operating system). In addition, where the development (or distribution to the public) of circumvention technology itself constitutes copyright infringement, the DMCA expressly precludes reliance on § 1201(f)(2) and (3). *See id.* (holding that "[t]he right to make the information available extends only to dissemination 'solely for the purpose' of

achieving interoperability as defined in the statute. It does not apply to public dissemination of means of circumvention") (footnote omitted).

Moreover, legislative history suggests that the "independently created [computer] program" referenced in this exemption must not infringe the original computer program and instead must be "a new and original work." H.R. Rep. No. 105-551 (II), at 42 (1998). Thus, if the defendant's functionally equivalent computer program is "new and original" only insofar as it lacks the original's access controls, then the defendant has not created an "independently created computer program." *Davidson*, 334 F. Supp. 2d at 1185, *aff'd*, 422 F.3d at 642. If, on the other hand, the defendant's program actually performs functions that the original program did not, courts are more inclined to find that defendants have satisfied the "independently created computer program" requirement. *Lexmark*, 387 F.3d at 550 (holding that even though remanufacturer's toner cartridge chip contained "exact copies" of original manufacturer's computer program, it was nonetheless an "independently created computer program" because it "contain[s] other functional computer programs beyond the copied" original program). The independent program need not have already existed before the defendant reverse-engineered the original program. *Id.* at 550-51 (holding that "nothing in the statute precludes simultaneous creation of an interoperability device and another computer program" so long as it is "'independently' created").

6. Encryption Research

Certain encryption research is exempted from liability under § 1201(a) (but *not* from § 1201(b)). *Reimerdes*, 111 F. Supp. 2d at 321 n.154. For purposes of this exemption, "encryption research" consists of "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products." 17 U.S.C. § 1201(g)(1)(A). The phrase, "encryption technologies," "means the scrambling and descrambling of information using mathematical formulas or algorithms." 17 U.S.C. § 1201(g)(1)(B).

The first encryption research exemption is that it is not a violation of the anti-circumvention provision (§ 1201(a)(1)(A)) where a defendant "circumvent[s] a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if" four conditions are satisfied: (1) he "lawfully

obtained" the applicable encrypted published work; (2) the circumvention "is necessary to conduct such encryption research;" (3) he "made a good faith effort to obtain authorization before the circumvention;" and (4) the circumvention does not constitute copyright infringement "or a violation of applicable law," including the Computer Fraud Abuse Act of 1986, 18 U.S.C. § 1030. 17 U.S.C. § 1201(g)(2).

To determine whether a defendant qualifies for this exemption, courts consider the following non-exclusive factors: (1) whether the results of the putative encryption research are disseminated in a manner designed to advance the state of knowledge of encryption technology versus facilitation of copyright infringement; (2) whether the person in question is engaged in legitimate study of or work in encryption; and (3) whether the results of the research are communicated in a timely fashion to the copyright owner. 17 U.S.C. § 1201(g)(3); *see also Reimerdes*, 111 F. Supp. 2d at 321.

The second encryption research exemption is that a defendant does not violate the access control anti-trafficking provision (§ 1201(a)(2)) for developing and distributing tools, such as software, that are needed to conduct permissible encryption research as described in the first encryption research exemption in § 1201(g)(2). 17 U.S.C. § 1201(g)(4); H.R. Rep. No. 105-551 (II), at 44 (1998). This exemption essentially frees an encryption researcher to cooperate with other researchers, and it also allows one researcher to provide the technological means for such research to another to verify the research results. *Id.*

It is not a violation of § 1201(a)(2) for a person to (1) "develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in" § 1201(g)(2) and (2) "provide the technological means to another person with whom he or she is working collaboratively" for the purpose of either conducting good faith encryption research or having another person verify such research as described in § 1201(g)(2). 17 U.S.C. § 1201(g)(4).

This exemption is quite complex and has been relied upon infrequently in reported decisions. For a report on the early effects of this exemption (or lack thereof) on encryption research and on protection of content owners against unauthorized access of their encrypted copyrighted works, see the "*Report to Congress: Joint Study of Section 1201(g) of The Digital Millennium Copyright Act*" prepared by the U.S. Copyright Office and the National Telecommunications

and Information Administration of the Department of Commerce pursuant to § 1201(g)(5), *available at* http://www.copyright.gov/reports/studies/dmca_report.html.

7. Restricting Minors' Access to the Internet

Section 1201(h) creates a discretionary exception, giving the court discretion to waive violations of § 1201(a)(1)(A) and 1201(a)(2) so that those prohibitions are not applied in a way that "inadvertently make[s] it unlawful for parents to protect their children from pornography and other inappropriate material available on the Internet, or have unintended legal consequences for manufacturers of products designed solely to enable parents to protect their children." H.R. Rep. No. 105-551 (II), at 45 (1998). Specifically, § 1201(h) authorizes the court to "consider the necessity for its intended and actual incorporation in a technology, product, service, or device, which (1) does not itself violate the provisions of this title; and (2) has the sole purpose to prevent the access of minors to material on the Internet." 17 U.S.C. § 1201(h). Congress was concerned that if Internet filtering tools are developed in the future that incorporate a part or component that circumvent access controls to a copyrighted work "solely in order to provide a parent with the information necessary to ascertain whether that material is appropriate for his or her child, this provision authorizes a court to take into consideration the necessity for incorporating such part or component in a suit alleging a violation of section 1201(a)." S. Rep. No. 105-190, at 14 (1998).

To date, no reported case has applied this discretionary exception.

8. Protection of Personally Identifying Information

Section 1201(i)(1) states that it is not a violation of § 1201(a)(1)(A) to circumvent an access control for the purpose of disabling files that collect personally identifiable information like "'cookie files'—which are automatically deposited on hard drives of computers of users who visit World Wide Web sites." *Id.* at 18. However, if a copyright owner conspicuously discloses that its access control also contains personal data gathering capability, and if the consumer is given the ability to effectively prohibit that gathering or dissemination of personal information, then this exception does not apply and no circumvention is permitted. H.R. Rep. No. 105-551 (II), at 45 (1998). Further, if the copyright owner conspicuously discloses that neither the access control nor the work it protects collect personally identifying information,

then no circumvention is permitted. 17 U.S.C. § 1201(i)(2). Note that this exception does not apply to the anti-trafficking prohibitions.

9. Security Testing

A person who engages in good faith "security testing" does not violate § 1201(a). 17 U.S.C. § 1201(j). "Security testing" consists of "accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network." 17 U.S.C. § 1201(j)(1). Without such authorization, a defendant cannot qualify for this exemption. *Reimerdes*, 111 F. Supp. 2d at 321. A defendant engaging in security testing does not violate § 1201(a)(1)(A) so long as such testing does not constitute copyright infringement nor a violation of other applicable law such as the Computer Fraud and Abuse Act of 1986. 17 U.S.C. § 1201(j)(2). In evaluating this exemption, the DMCA requires a court to consider whether the information derived from the security testing (1) "was used solely to promote the security of the owner or operator of [or shared directly with the developer of] such computer, computer system or computer network, or" (2) "was used or maintained in a manner that does not facilitate [copyright] infringement" or a violation of other applicable law. 17 U.S.C. § 1201(j)(3).

Likewise, a defendant does not violate § 1201(a)(2) for trafficking in a "technological means for the sole purpose of performing the acts of security testing" if the testing does not "otherwise violate section (a)(2)." 17 U.S.C. § 1201(j)(4).

10. Constitutionality of the DMCA

Civil and criminal defendants have repeatedly challenged the constitutionality of Title I of the DMCA, particularly 17 U.S.C. § 1201(a)(2) and 1201(b). Defendants have repeatedly challenged Congress's authority, for example, to enact the DMCA pursuant to the Commerce Clause and Intellectual Property Clause. None of these challenges has yet prevailed.

a. Congress's Constitutional Authority to Enact § 1201 of the DMCA

Congress enacted § 1201 pursuant to its authority under the Commerce Clause. *See* U.S. Const., art. I, § 8, cl. 3; H.R. Rep. No. 105-551 (II), at 22, 35 (1998). Federal courts have uniformly upheld this authority. *See*, *e.g.*, *United*

States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1138 (N.D. Cal. 2002) ("Congress plainly has the power to enact the DMCA under the Commerce Clause."); *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1103 (N.D. Cal. 2004) (same). Article I, Section 8, Clause 3 of the Constitution delegates to Congress the power "[t]o regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes." Congress does not exceed its Commerce Clause authority where a rational basis exists "for concluding that a regulated activity sufficiently affected interstate commerce." *United States v. Lopez*, 514 U.S. 549, 558 (1995) (citations omitted). The DMCA prohibits circumventing access controls and the trafficking in technology that facilitates circumvention of access or copy controls—the type of conduct that has a substantial effect on commerce between the states and commerce with foreign nations. *See 321 Studios*, 307 F. Supp. 2d at 1103. Congress created the DMCA's anti-trafficking prohibitions to directly regulate specific items moving in commerce (circumvention technology) and to protect channels of interstate commerce, including electronic commerce. H.R. Rep. No. 105-551(II), at 22 (1998). Most significantly, to the extent that circumvention devices enable criminals to engage in piracy by unlawfully copying and distributing copyrighted works, the sale of such devices has a direct effect on suppressing the market for legitimate copies of the works. *See 321 Studios*, 307 F. Supp. 2d at 1103; *Elcom*, 203 F. Supp. 2d at 1138. Accordingly, Congress had a rational basis for concluding that § 1201 regulates activity that substantially affects interstate commerce and therefore acted within its authority under the Commerce Clause. *See Elcom*, 203 F. Supp. 2d at 1138.

Courts have similarly rejected the argument that the DMCA violates the Intellectual Property Clause. The Commerce Clause authorizes Congress to enact legislation that protects intellectual property rights, even where the Intellectual Property Clause alone does not provide sufficient authority for such legislation. Federal courts have long recognized that while each of the powers of Congress is alternative to all of the others, "what cannot be done under one of them may very well be doable under another." *United States v. Moghadam*, 175 F.3d 1269, 1277 (11th Cir. 1999). Congress may thus use the Commerce Clause as a basis for legislating within a context contemplated by another section of the Constitution (like the Intellectual Property Clause) so long as Congress does not override an otherwise existing Constitutional limitation. *Id.* (holding the criminal anti-bootlegging statute, 18 U.S.C. § 2319A, valid under the Commerce Clause even if it is beyond Congress's authority under the Intellectual Property Clause); *compare Heart of Atlanta Motel v. United*

States, 379 U.S. 241 (1964) (upholding public accommodation provisions of the Civil Rights Act of 1964 as valid under the Commerce Clause despite the fact that the Act may have reached beyond Congress's authority under the Fourteenth Amendment), *and South Dakota v. Dole*, 483 U.S. 203, 207 (1987) (holding that Congress could rely on the Spending Clause to impose restrictions that would otherwise exceed Congress's power), *with Railway Labor Executives' Ass'n v. Gibbons*, 455 U.S. 457 (1982) (striking down act by Congress under Commerce Clause that violated Bankruptcy Clause's uniformity requirement). Further, the Intellectual Property Clause "itself is stated in positive terms, and does not imply any negative pregnant" that would suggest "a ceiling on Congress' ability to legislate pursuant to other grants." *Moghadam*, 175 F.3d at 1280 (discussing constitutionality of the criminal anti-bootlegging statute, 18 U.S.C. § 2319A). Moreover, "[e]xtending quasi-copyright protection also furthers the purpose of the Copyright Clause to promote the progress of the useful arts." *Id.*

The DMCA's enactment pursuant to the Commerce Clause was valid because it "is not fundamentally inconsistent with" the purpose of the Intellectual Property Clause. *Elcom*, 203 F. Supp. 2d at 1139-41. Indeed, Congress "viewed the [DMCA] legislation as 'paracopyright' legislation that could be enacted under the Commerce Clause." *Id.* at 1140. Moreover, protecting copyright owners' rights against unlawful piracy by preventing trafficking in tools that would enable widespread piracy and unlawful infringement (i.e., circumvention tools) is consistent with the Intellectual Property Clause's grant to Congress of the power to "'promote the useful arts and sciences' by granting exclusive rights to authors in their writings." *Id.*

Specifically, courts have rejected the common argument that the DMCA's ban on the sale of circumvention tools violates the Intellectual Property Clause's "limited Times" prohibition. That argument is based on the false premise that the DMCA has the effect of allowing publishers to claim copyright-like protection in copyrighted works, even after they pass into the public domain. Prosecutors should vigorously oppose this flawed argument. Nothing in the DMCA permits a copyright owner to prevent his work from entering the public domain, despite the expiration of the copyright. *Id.* at 1141. As discussed in the copyright chapter, the essence of copyright is the legally enforceable exclusive right to reproduce and distribute copies of an original work of authorship, to make derivative works, and to perform the work publicly for a limited time. *See supra* Chapter II; *see also Elcom*, 203 F. Supp. 2d at 1141; 17 U.S.C. §§ 106,

302, 303. When a copyright expires, so does any protectable intellectual property right in a work's expression. *Elcom*, 203 F. Supp. 2d at 1141. Upon expiration, the user may copy, quote, or republish the expression without any legally enforceable restriction on the use of the expression. *Id.* "Nothing within the DMCA grants any rights to anyone in any public domain work. A public domain work remains in the public domain[,] and any person may make use of the public domain work for any purpose." *321 Studios*, 307 F. Supp. 2d at 1104 (internal quotation marks and citation omitted). Accordingly, the DMCA does not extend any copyright protections beyond the statutory copyright term merely by prohibiting the trafficking in or marketing of circumvention technology. *Id.*

b. The First Amendment

Criminal and civil DMCA defendants have raised both facial and "as applied" First Amendment challenges. Although federal courts have uniformly rejected such challenges, defendants continue to raise them in part because the overbreadth and "as applied" First Amendment tests each can include a fact-dependent component.

i. Facial Challenges

Facial First Amendment challenges to § 1201—typically alleging that the statute is unconstitutionally overbroad—fail for at least two reasons. First, the DMCA does not expressly proscribe spoken words or patently expressive or communicative conduct. *See Roulette v. City of Seattle*, 97 F.3d 300, 303 (9th Cir. 1996). "[A] facial freedom of speech attack must fail unless, at a minimum, the challenged statute is directed narrowly and specifically at expression or conduct commonly associated with expression." *Id.* at 305 (citations and internal quotation marks omitted); *see also Virginia v. Hicks*, 539 U.S. 113, 123 (2003).

Section 1201 of the DMCA, "[b]y its terms," is not directed at expression or conduct associated with expression. *Elcom*, 203 F. Supp. 2d at 1133. Instead, § 1201 is a law of general application focused on the circumvention of access controls and the trafficking in circumvention tools; § 1201's prohibitions are not focused on speech. *Id.*; *see also Anderson v. Nidorf*, 26 F.3d 100, 103-04 (9th Cir. 1994) (holding that California's anti-piracy statute is not subject to facial challenge because, *inter alia*, the statute focused upon infringement for commercial advantage or private financial gain). Accordingly, on this basis

alone, "an overbreadth facial challenge [to § 1201] is not available." *Elcom*, 203 F. Supp. 2d at 1133.

Second, even were the DMCA directed at spoken words or expressive conduct—which no court has yet held—such a finding would be insufficient to establish overbreadth as a matter of law. The defendant would still have to independently establish that the DMCA is written so broadly that it infringes unacceptably on the First Amendment rights of third parties. *City Council v. Taxpayers for Vincent*, 466 U.S. 789, 798-99 (1984). The overbreadth doctrine "is, manifestly, strong medicine," to be employed "sparingly and only as a last resort." *Broadrick v. Oklahoma*, 413 U.S. 601, 613 (1973). For this reason, a statute will be declared facially unconstitutional for overbreadth only if the court finds a realistic danger that the statute itself will significantly compromise recognized First Amendment protections of parties not before the court. *See New York State Club Ass'n, Inc. v. City of New York*, 487 U.S. 1, 11 (1988).

The DMCA neither compromises a recognized First Amendment protection of third parties, nor is there a realistic danger that such a compromise would occur. Moreover, § 1201's "plainly legitimate sweep" targets circumvention of access controls and the manufacture or trafficking in circumvention technology, not speech. Thus, it is highly unlikely that defendants could establish the facts necessary to claim that § 1201 is overbroad. *See Elcom*, 203 F. Supp. 2d at 1133.

ii. "As Applied" Challenges

First Amendment "as applied" challenges to § 1201 necessarily vary according to the technology at issue in each defendant's particular case. DMCA defendants have often alleged that the DMCA violates the First Amendment when applied to circumvention technology in the form of computer code. Although it is arguable whether computer object code constitutes speech, every federal court that has held that computer code is speech has nonetheless ruled that the anti-trafficking provisions do not violate the First Amendment under an intermediate scrutiny standard because the DMCA (1) is content-neutral; (2) furthers important governmental interests in promoting electronic commerce and protecting the rights of copyright owners; and (3) is sufficiently tailored to achieve these objectives without unduly burdening free speech. *See, e.g., Elcom*, 203 F. Supp. 2d at 1126-28 (applying *United States v. O'Brien*, 391 U.S. 367, 376 (1968) ("When 'speech' and 'nonspeech' elements are combined in the same course of conduct, a sufficiently important governmental interest

in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms.")).

The DMCA's anti-trafficking provisions are content neutral. *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 454 (2d Cir. 2001) (§ 1201(a)(2)); *321 Studios*, 307 F. Supp. 2d at 1100 (§ 1201(a)(2) and 1201(b)); *Elcom*, 203 F. Supp. 2d at 1128-29 (§ 1201(b)). The principal inquiry in determining whether a statute is content neutral is "'whether the government has adopted a regulation of speech because of [agreement or] disagreement with the message it conveys.'" *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 642 (1994) (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989)). The government's purpose is the controlling measure. *Id.*

By this measure, the DMCA's anti-trafficking provisions are clearly content-neutral. Congress intended the DMCA to target the non-speech, functional components of circumvention technology, *Corley*, 273 F.3d at 454, not to "stifle[] speech on account of its message." *Turner*, 512 U.S. at 641. The DMCA is not a content-based statute that would require strict scrutiny under the First Amendment. *See 321 Studios*, 307 F. Supp. 2d at 1100. In fact, "[t]he reason that Congress enacted the anti-trafficking provision of the DMCA had nothing to do with suppressing particular ideas of computer programmers and everything to do with functionality." *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 329 (S.D.N.Y. 2000), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

Ultimately, the DMCA is not concerned with whatever capacity circumvention technology might have for conveying information to a person, and that capacity is what arguably creates the speech component of, for example, decrypting computer code. *See Corley*, 273 F.3d at 454. The DMCA would apply to such code solely because of its capacity to decrypt, for instance, an access control. *Id.* "That functional capability is not speech within the meaning of the First Amendment." *Id.*

A statute that is content neutral is subject to intermediate scrutiny and hence satisfies the First Amendment "if it furthers an important or substantial government interest; if the government interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." *Turner*, 512 U.S. at 662 (quotation and citation omitted). The government's interest in preventing unauthorized copying of copyrighted works and

promoting electronic commerce are unquestionably substantial. *See* H.R. Rep. No. 105-551 (II), at 23 (1998); *Elcom*, 203 F. Supp. 2d at 1129-30; *Corley*, 273 F.3d at 454. Congress enacted the DMCA after evaluating a great deal of evidence establishing that copyright and intellectual property piracy are endemic, especially digital piracy. *See* S. Rep. No. 105-190, at 8 (1998). Thus, by prohibiting circumvention of access controls and the trafficking in circumvention technology, "the DMCA does not burden substantially more speech than is necessary to achieve the government's asserted goals of promoting electronic commerce, protecting copyrights, and preventing electronic piracy." *See 321 Studios*, 307 F. Supp. 2d at 1103 (internal quotation marks and citation omitted).

Finally, courts have uniformly found that the DMCA's anti-trafficking provisions meet the Supreme Court's narrow tailoring requirement that a content-neutral regulation of speech promote a substantial government interest that would be achieved less effectively absent the regulation. *See id.* at 1101. The DMCA's numerous exceptions (see Section C. of this Chapter) further demonstrate that Congress narrowly tailored the statute to balance, for instance, the needs of law enforcement, computer programmers, encryption researchers, and computer security specialists against the problems created by circumvention technology. *See* 17 U.S.C. § 1201(e)-(g), (j); *Elcom*, 203 F. Supp. 2d at 1130-31.

c. Vagueness

Courts have also rejected challenges to the DMCA under the Fifth Amendment on vagueness grounds. Vagueness may invalidate a statute if the statute either (1) fails to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits, or (2) authorizes or encourages arbitrary and discriminatory enforcement. *City of Chicago v. Morales*, 527 U.S. 41, 56 (1999). Defendants typically argue that the DMCA is vague or otherwise infirm because it bans only those circumvention tools that are primarily designed to circumvent access or copy controls to enable copyright infringement, not those enabling fair uses. *See*, *e.g., Elcom*, 203 F. Supp. 2d at 1122. This issue has arisen with respect to § 1201(b), which prohibits trafficking in any copy control circumvention technology. *Id.* at 1124.

Courts have held, however, that the DMCA is not unconstitutionally vague, because it imposes a blanket ban on all circumvention tools regardless of whether the ultimate purpose for their use is fair or infringing. *Id.* "Congress

thus recognized that most uses of tools to circumvent copy restrictions would be for unlawful infringement purposes rather than for fair use purposes and sought to ban all circumvention tools that 'can be used' to bypass or avoid copy restrictions." *Id.* at 1125 (quoting S. Rep. No. 105-190, at 29-30). Moreover, Congress's intent to preserve fair use, *see* § 1201(c), is not inconsistent with a ban on trafficking in circumvention technologies, even those that could be used for fair use purposes rather than infringement. *Elcom*, 203 F. Supp. 2d at 1125. Although the DMCA may make certain fair uses in digital works more difficult, the DMCA does not eliminate fair use and in fact expressly permits it. *See Elcom*, 203 F. Supp. 2d at 1125; 17 U.S.C. § 1201(c)(1). "Thus, while it is not unlawful to circumvent for the purpose of engaging in fair use, it is unlawful to traffic in tools that allow fair use circumvention." *Elcom*, 203 F. Supp. 2d at 1125. Further, because the DMCA prohibits the trafficking of all circumvention tools, Congress need not expressly tie the use of the tool to an unlawful purpose (as may be required, for instance, in a multi-use device context). *Id.* Accordingly, the DMCA, "as written, allows a person to conform his or her conduct to a comprehensible standard and is thus not unconstitutionally vague." *Id.* (citation omitted).

d. Fair Use

For a more detailed explanation of the fair use doctrine, see Section C.5. of Chapter II of this Manual.

Defendants typically style their fair use defense to a DMCA violation as an "as applied" First Amendment challenge. For example, traffickers have raised fair use challenges "as applied" to the First Amendment rights of third-party purchasers of the trafficker's circumvention tools. This type of fair use defense fails for at least three reasons. First, the challengers usually lack standing. "[A] person to whom a statute may constitutionally be applied will not be heard to challenge that statute on the ground that it may conceivably be applied unconstitutionally to others, in other situations not before the Court." *Broadrick v. Oklahoma*, 413 U.S. 601, 610 (1973). Those who traffic in circumvention tools that they do not use cannot assert a fair use defense because they are not engaging in any use—fair or infringing—of a copyrighted work. Simply put, traffickers lack standing to challenge the DMCA's constitutionality based on its application to the traffickers' customers.

Second, even a purchaser who could have standing because he did use a copyrighted work cannot rely on the fair use defense, because the DMCA does

not present an issue of infringement. Fair use is an affirmative defense to copyright infringement, something that the user can accomplish only *after* he has first circumvented a work's copy controls. *See*, *e.g.*, *Elcom*, 203 F. Supp. 2d at 1121. The DMCA "targets the circumvention of digital walls guarding copyrighted material (and trafficking in *circumvention* tools), [it] does not concern itself with the *use* of those materials after circumvention has occurred." *Corley*, 273 F.3d at 443; *United States v. Crippen*, No. CR09-703PSG, 2010 WL 7198205, at *2 (C.D. Cal. Nov. 23, 2010) (same) (granting the government's motion in limine to exclude evidence of fair use at trial where defendant was charged with DMCA violations for modifying Microsoft Xbox gaming systems); *see also MGE UPS Sys., Inc. v. GE Consumer and Ind., Inc.*, 622 F.3d 361, 366 (5th Cir. 2010) ("Because § 1201(a)(1) is targeted at circumvention, it does not apply to the use of copyrighted works *after* the technological measure has been circumvented."). Thus, the DMCA's anti-trafficking provisions are not concerned with purchasers' downstream use of circumvention tools. *See Corley*, 273 F.3d at 442; *Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 943-44 (N.D. Cal. 2009); *321 Studios*, 307 F. Supp. 2d at 1097-98.

Third, no court has held that the fair use doctrine is a categorical constitutional requirement. *Corley*, 273 F.3d at 458 ("[T]he Supreme Court has never held that fair use is constitutionally required."). Fair use is a judicially-created doctrine. *Reimerdes*, 111 F. Supp. 2d at 321. Fair use existed only at common law until Congress codified it in the 1976 Copyright Act at 17 U.S.C. § 107, in order to maintain the common-law status quo. *See* H.R. Rep. No. 94-1476, at 66 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5680.

The fact that the fair use doctrine accommodates First Amendment protections—i.e., that certain fair uses may also be protected under the First Amendment, *cf. Eldred v. Ashcroft*, 537 U.S. 186, 218-20 (2003); *Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 560 (1985)—does not make the fair use doctrine and the First Amendment categorically coextensive. *See Elcom*, 203 F. Supp. 2d at 1134 n.4 ("[There] is no direct authority for the proposition that the doctrine of fair use is coextensive with the First Amendment, such that 'fair use' is a First Amendment right").

Most significantly, courts have rejected "the proposition that fair use, as protected by the Copyright Act, much less the Constitution, guarantees copying by the optimum method or in the identical format of the original." *Corley*, 273 F.3d at 459. Fair use of copyrighted digital works is still possible under the

DMCA, even though copying of such works may prove more difficult. *321 Studios*, 307 F. Supp. 2d at 1102.

In addition, the DMCA does not place an impermissible financial burden on fair users' First Amendment rights. Courts have found that this "financial burden" argument "is both an overstatement of the extent of the fair use doctrine and a misstatement of First Amendment law." *Id.* A statute's financial burden on a speaker renders the statute unconstitutional only if such burden was placed on the speaker because of the speech's content, not because of the speaker's desire to make the speech. *Id.* (citations omitted). Section 1201 of the DMCA does not eliminate fair use nor prevent anyone from engaging in traditional methods of fair use such as "quoting from a work or comparing texts for the purpose of study or criticism." *Elcom*, 203 F. Supp. 2d at 1134.

Finally, courts have rejected the argument that the DMCA impairs an alleged First Amendment fair use right to access non-copyrighted works in the public domain, because the DMCA permits authors to use access and copy controls to protect non-copyrighted works and copyrighted works alike. *See*, *e.g., 321 Studios*, 307 F. Supp. 2d at 1102; *Elcom*, 203 F. Supp. 2d at 1134. Neither the DMCA nor the presence of access or copy controls affect whether or not a work is in the public domain. *321 Studios*, 307 F. Supp. 2d at 1102.

D. Penalties

For the first criminal violation of Title I of the DMCA (§§ 1201, 1202), the maximum penalty is five years' imprisonment, a $500,000 fine or twice the monetary gain or loss, or both imprisonment and a fine. 17 U.S.C. §§ 1204, 3571(d). For subsequent offenses, the maximum penalty is ten years' imprisonment, a $1 million fine or twice the monetary gain or loss, or both imprisonment and a fine. *Id*. For a more complete discussion of sentencing issues, see Chapter VIII of this Manual.

VI. Counterfeit and Illicit Labels, Counterfeit Documentation and Packaging—18 U.S.C. § 2318

A. Distinguished from Trademark and Copyright Statutes

Creative works can be protected by criminal laws other than the Copyright Act. The most important of these is 18 U.S.C. § 2318, which criminalizes knowingly trafficking in counterfeit or illicit labels and counterfeit documentation and packaging for certain types of copyrighted works. Although § 2318 regulates items that accompany copyrighted works, it is not a pure copyright statute, and its protections differ in scope from those afforded by the Copyright Act.

Section 2318 also differs from civil and criminal trademark law. Although counterfeit and illicit labels, documentation, and packaging often bear counterfeit trademarks (trafficking in which is prohibited by the criminal trademark statute, 18 U.S.C. § 2320), the use of a counterfeit mark is not an element of a § 2318 offense. Section 2318 also differs from § 2320 in the types of labels and packaging covered by each statute. Section 2320 criminalizes trafficking of labels and related labeling components bearing counterfeit trademarks, where such labels are used, designed, or intended to be used with any types of good or service, whereas § 2318 covers only counterfeit labels (as well as documentation and packaging) in connection with certain classes of copyrighted works.

Section 2318 originally addressed counterfeit labels for sound recordings, but has evolved over time to address counterfeit labels, documentation, and packaging for a broader class of copyrighted works. See Sections B.3., B.4., and E.5. of this Chapter. As a result of 2004 amendments, § 2318 now prohibits trafficking in counterfeit labels for movies, music, software, copies of literary, pictorial, graphic, or sculptural works, or works of visual art, or labels designed

to be used with documentation and packaging for any of the enumerated classes of copyrighted works. 18 U.S.C. § 2318(a)(1)(A). Section 2318 also prohibits trafficking in counterfeit documentation and packaging for the classes of works listed above. 18 U.S.C. § 2318(a)(1)(B). In 2006, Congress further expanded § 2318 to address trafficking in what are known as "illicit" labels, which are "genuine certificate[s], licensing document[s], registration card[s], or similar labeling component[s]" that the copyright owner would normally use to verify that a work is noninfringing (i.e., legitimate), but which are distributed or intended for distribution without the owner's permission, presumably to facilitate infringement. 18 U.S.C. § 2318(b)(4). In 2008, the PRO-IP Act revised § 2318's restitution provision to refer to 18 U.S.C. § 2323, the general forfeiture and restitution provision for IP offenses also created by the PRO-IP Act. 18 U.S.C. § 2318(d). The PRO-IP Act also renumbered the subsections within § 2318(a).

Sample indictments and jury instructions are provided in Appendix F of this Manual.

B. Elements

To obtain a conviction under 18 U.S.C. § 2318, the government must prove five elements:

1. The defendant acted knowingly
2. The defendant trafficked
3. In labels affixed to, enclosing, or accompanying (or designed to be affixed to, enclose, or accompany) a phonorecord, computer program, motion picture or other audiovisual work, literary, pictorial, graphic, or sculptural work, or work of visual art, or documentation or packaging for such works (i.e., trafficked either in documentation or packaging for such works itself, or in labels for such documentation or packaging)
4. The documentation or packaging were counterfeit, or the labels were counterfeit or illicit
5. Federal jurisdiction is satisfied because:
    a. the offense occurred in special maritime territories or other areas of special jurisdiction of the United States;
    b. the offense used or intended to use the mail or a facility of interstate or foreign commerce;

c. the counterfeit or illicit labels were affixed to, enclosed, or accompanied copyrighted materials (or were designed to); or
d. the documentation or packaging is copyrighted.

These elements are reviewed in detail in the following sections.

1. The Defendant Acted "Knowingly"

Section 2318 is a general intent crime. The government must prove first that the defendant acted "knowingly." This is less difficult than proving that the defendant acted willfully, as with criminal copyright cases. See Chapter II, Section B.2. of this Manual for a discussion of the "willful" standard in criminal copyright infringement cases. Proving knowledge under § 2318 requires the government to show only that the defendant knew that he was taking the actions described in the statute. The government does not have to show that the defendant knew his conduct was illegal. *See Bryan v. United States*, 524 U.S. 184, 193 (1998) (firearms offense) ("'[K]nowingly' merely requires proof of knowledge of the facts that constitute the offense.").

To establish knowledge in § 2318 cases involving counterfeit labels, the government does not have to prove that the defendant acted with fraudulent intent. Congress eliminated that element in 1982, believing that such proof was "superfluous" because the government must already prove that the defendant knew his labels were counterfeit. S. Rep. No. 97-274, at 9 (1981), *reprinted in* 1982 U.S.C.C.A.N. 127, 135 ("In other words, it would be difficult to conceive of a situation in which one could traffic in articles knowing that they are counterfeit without intending to defraud the purchaser."). It is less clear whether, and to what extent, a requirement of fraudulent intent may be assumed in cases involving illicit labels, but the statute does not expressly require such proof. Nonetheless, the government must prove that the defendant knew that the labels, documentation, or packaging in which he trafficked were counterfeit or illicit. *See, e.g.*, *United States v. Teh,* 535 F.3d 511, 519-20 (6th Cir. 2008)*; United States v. Dixon*, No. 84-5287, 1985 U.S. App. LEXIS 27076, at *9-11 (4th Cir. Aug. 12, 1985); *see also Microsoft Corp. v. Pronet Cyber Techs., Inc.*, 593 F.Supp.2d 876, 884 (E.D. Va. 2009) ("[Section] 2318's legislative history suggests that Congress was well aware that the amended statute only required proof of knowledge that labels were counterfeit—namely, that the labels appeared to be genuine, but were not.").

It may also suffice to prove that the defendant was willfully blind to the fact that the items trafficked were counterfeit or illicit. Although no published

cases specify that the government may satisfy § 2318 through proof of willful blindness (also known as "conscious avoidance" or deliberate ignorance), courts have held that proving willful blindness generally suffices to prove knowledge in criminal cases. *See United States v. Jewell*, 532 F.2d 697, 699-704 (9th Cir. 1976) (discussing the history and use of "deliberate ignorance" instructions); *Microsoft Corp. v. Compusource Distribs., Inc.*, 115 F. Supp. 2d 800, 808-09 (E.D. Mich. 2000) (citing evidence of defendant's willful blindness as to authenticity of software as supporting finding that he knew software was counterfeit); *see also* Deborah Sprenger, *Propriety of Instruction of Jury on "Conscious Avoidance" of Knowledge of Nature of Substance or Transaction in Prosecution for Possession or Distribution of Drugs*, 109 A.L.R. Fed. 710 § 2[a] (2005). "The knowledge element of a crime such as the one charged here may be satisfied upon a showing beyond a reasonable doubt that a defendant had actual knowledge or deliberately closed his eyes to what otherwise would have been obvious to him concerning the fact in question." *United States v. Brodie*, 403 F.3d 123, 148 (3d Cir. 2005) (internal quotation marks and citation omitted) (Trading with the Enemy Act of 1917 and Cuban Assets Control Regulations violations). Willful blindness goes beyond negligence: the defendant himself must have been "objectively aware of the high probability of the fact in question, and not merely that a reasonable man would have been aware of the probability." *Id.* (internal quotation marks and citation omitted).

The government need not prove that the defendant knew that his conduct met the jurisdictional elements listed in § 2318(c), such as that the computer program to which he had affixed his counterfeit labels was copyrighted. See Section B.5. of this Chapter.

2. The Defendant Trafficked

In the second element of a § 2318 offense, the government must prove that the defendant trafficked in labels, documentation, or packaging. The term "traffic" in § 2318 is defined by reference to the definition of "traffic" used in § 2320. *See* 18 U.S.C § 2320(f)(5) ("the term 'traffic' means to transport, transfer, or otherwise dispose of, to another, for purposes of commercial advantage or private financial gain, or to make, import, export, obtain control of, or possess, with intent to so transport, transfer, or otherwise dispose of."). See also Chapter III, Section B.3. of this Manual for a discussion of the term "traffic" as an element of a § 2320 offense. The only difference to note between the application of the term traffic in § 2318 and § 2320 is that § 2320 punishes attempts whereas § 2318 does not, and therefore any discussion of attempted

trafficking with regard to § 2320 may not apply to § 2318. On the other hand, because the definition of "traffic" in both statutes includes many acts that are preparatory to distributing contraband—such as making it, obtaining it, and possessing it with intent to traffic—the omission of an attempt provision in § 2318 should not prevent the government from pursuing otherwise deserving cases. Thus, labels seized during the search of a counterfeiting operation may constitute part of the indicted conduct, whether or not the labels had yet been affixed to the works or transferred to distributors or customers.

3. Trafficking in Labels Affixed to, Enclosing, or Accompanying (or Designed to be Affixed to, Enclose, or Accompany) a Phonorecord, Computer Program, Motion Picture or Other Audiovisual Work, Literary, Pictorial, Graphic, or Sculptural Work, or Work of Visual Art, or Trafficking in Documentation or Packaging for Such Works

In the third element of a § 2318 offense, the government must prove that the labels in which the defendant trafficked were affixed to, enclosing, or accompanying—or designed to be affixed to, enclose, or accompany—phonorecords, motion pictures or other audiovisual works, computer software, literary, pictorial, graphic, or sculptural works, or works of visual art. *See* 18 U.S.C. § 2318(a)(1)(A), (b)(3) (defining the classes of copyrighted works); 17 U.S.C. §§ 101, 102 (same). Alternatively, the government may show that the defendant trafficked in documentation or packaging for one of the enumerated class of works, or labels affixed or designed to be affixed to copyrighted documentation and packaging. *See* 18 U.S.C. § 2318(a)(1)(B), (b)(5).

The types of copyrighted works covered by the statute has expanded significantly over the past two decades. Before 2004, 18 U.S.C. § 2318 applied only to labels for movies, music, and software, and to documentation and packaging only for computer software. The provisions relating to computer software were added in 1996. As of 2004, however, § 2318 applies to labels, documentation, and packaging for most types of copyrighted works that are capable of being labeled or packaged. *See* 18 U.S.C. § 2318(a)(1), (b)(5).

Counterfeit labels (or documentation or packaging) need not actually be affixed or attached to a copyrighted work to support a § 2318 charge, but rather, need only be "affixed to, enclosing, or accompanying, or *designed to be* affixed to, enclose, or accompany." 18 U.S.C. § 2318(a)(1) (emphasis added). Nevertheless, some nexus between the labels (or documentation or packaging) and copyrighted works—whether actual or intended—is still required.

Documentation and packaging still need only be "for" the enumerated classes of copyrighted works. 18 U.S.C. § 2318(b)(5). Given the context, the word "for" appears to have roughly the same meaning for documentation and packaging that "affixed to, enclosing, or accompanying, or designed to be affixed to, enclose, or accompany" has for labels. Thus, some physical nexus with copyrighted works—whether actual or intended—is required for documentation and packaging as well.

For a discussion of whether § 2318 applies to labels, documentation, and packaging in electronic form, see Section D.1. of this Chapter.

4. The Labels, Documentation, or Packaging Materials Are Counterfeit or Illicit

In the fourth element, the government must prove that the packaging or documentation is "counterfeit" or that the labels are "counterfeit" or "illicit." *See* 18 U.S.C. § 2318(a)(1)(A)-(B). "Counterfeit" is defined as something "that appears to be genuine, but is not." 18 U.S.C. § 2318(b)(1), (b)(6). Courts have determined labels to be counterfeit for purposes of § 2318 where, for example, a defendant created the labels to accompany or apply to copies of Microsoft products and reprinted a Microsoft product key for a different copy on the label, *Microsoft Corp. v. Pronet Cyber Techs., Inc.*, 593 F. Supp. 2d 876, 882 (E.D. Va. 2009); and where DVD labels "appeared to be 'home made[,]' were of poor quality, contained misspellings, and were not centered," *United States v. Teh*, 535 F.3d 511, 520 (6th Cir. 2008).

Counterfeit is distinct from "bootlegged" or "pirated" in that counterfeits are unauthorized copies of works that are made to appear legitimate, whereas bootlegged recordings or pirated items do not pretend to be legitimate. *See United States v. Shultz*, 482 F.2d 1179, 1180 (6th Cir. 1973) ("Counterfeit tapes are tapes which are represented to be genuine articles of particular record companies when, in truth, they are not. The process includes reproducing the tape itself and also the recognized label of another record company. A bootleg tape is a reproduction of someone else's recording or recordings marketed under a different label."). *See also* 18 U.S.C. § 2319A (addressing the unauthorized recording and trafficking of live musical performances, also known as "bootlegging"); Chapter II of this Manual.

Counterfeit labels include those made when "counterfeiters have simulated 'genuine' labels that have not previously existed," insofar as these simulated labels share the same basic criminal purpose as any counterfeit product—

to defraud the consumer, the manufacturer, and society by trading off the product's apparent authenticity. *See* S. Rep. No. 97-274, at 9 (1981), *reprinted in* 1982 U.S.C.C.A.N. 127, 135. "For example, cases have arisen where a counterfeiter has produced packages and distributed videotapes of a film which have never been released in that form to the public. The term 'counterfeit label' includes such simulated labels." *Id.* Except for the *Shultz* case, *supra*, the extent to which such simulated labels are counterfeit for purposes of § 2318 has rarely been addressed in the courts. Prosecutors handling cases involving simulated labels may find it helpful to consult with the Computer Crime and Intellectual Property Section at (202) 514-1026.

An "illicit" label, generally speaking, is a "genuine certificate, licensing document, registration card, or similar labeling component" intended for use with one of the enumerated classes of copyrighted works, that a defendant distributed or used without the work it was intended to accompany or falsely altered to indicate broader rights than originally intended. 18 U.S.C. § 2318(b)(4). Specifically, an "illicit" label is one that is:

> (A) used by the copyright owner to verify that [a copyrighted work of the type enumerated above] is not counterfeit or infringing of any copyright; and
> (B) that is, without the authorization of the copyright owner [either]—
> (i) distributed or intended for distribution not in connection with the copy, phonorecord, or work of visual art to which such labeling component was intended to be affixed by the respective copyright owner; or
> (ii) in connection with a genuine certificate or licensing document, knowingly falsified in order to designate a higher number of licensed users or copies than authorized by the copyright owner, unless that certificate or document is used by the copyright owner solely for the purpose of monitoring or tracking the copyright owner's distribution channel and not for the purpose of verifying that a copy or phonorecord is noninfringing.

18 U.S.C. § 2318(b)(4). Under subsection (A), an illicit label may include any of a broad category of labeling components, such as most types of identifying labels, particularly those that include trademarks, seals, holograms, watermarks, or other marks intended to show that a product is genuine. Although it is not clear from the statute's text and legislative history, presumably the definition does not include generic labels, such as packing slips, that merely identify a

particular work, but which the copyright holder did not intend to certify the work's authenticity.

Subsection (B) identifies two situations in which a labeling component is "illicit." First, a labeling component is illicit when it is distributed, without the copyright holder's permission, apart from the original copyrighted item that the copyright owner intended the labeling component to accompany. For example, individual "licensing packs" for software that contain various labels, certificates of authenticity, and documentation and packaging would be deemed illicit if they were sold without the original media they were intended to accompany, or were sold with a pirated copy of the media.

Second, a genuine labeling component is illicit when a genuine certificate of authenticity or similar licensing document has been knowingly falsified to indicate a higher number of authorized users or copies. For example, business software often comes in multi-user license packs that contain a single copy of the software itself on CD-ROM and a license that permits the software to be run for a certain number of users. If the licensing document for a ten-user license pack were knowingly falsified to indicate authorization for 100 users, the falsified licensing document would be illicit.

5. Federal Jurisdiction

The final element of § 2318 requires the government to establish federal jurisdiction over the offense by proving any one of the following circumstances:

- The offense occurred in a special maritime, territorial, or aircraft jurisdiction of the United States, § 2318(c)(1)
- Use of or intent to use the mail or facilities of interstate or foreign commerce in the commission of the offense, § 2318(c)(2)
- In the case of a counterfeit or illicit label, the label was affixed to, enclosed, or accompanied or designed to be affixed to, enclose, or accompany certain copyrighted works or a copy of these works: a phonorecord of a copyrighted sound recording or musical work; a computer program; a literary work; a pictorial, graphic or sculptural work; a work of visual art; or copyrighted documentation or packaging, § 2318(c)(3)
- In the case of counterfeit documentation or packaging, the documentation or packaging itself was copyrighted, § 2318(c)(4)

These jurisdictional elements are listed disjunctively, and therefore any one will suffice to support a § 2318 charge. For example, where a defendant trafficked in counterfeit labels for DVDs, the jurisdictional basis for a § 2318

charge could be met by showing *either* that the labels were affixed (or designed to be affixed) to DVD copies of a copyrighted motion picture, *or* that the defendant used the mails or other facilities of interstate commerce to traffic in the labels, *or* that the defendant trafficked in the special maritime jurisdiction of the United States. In practice, the most likely basis for jurisdiction will be copyright. Even when the works are copyrighted, however, prosecutors may nevertheless find it easier to establish another basis for jurisdiction: a copyright may be more burdensome to prove or an alternative basis may be relatively clear. See Chapter II of this Manual, which discusses how to prove the existence of a copyright.

The jurisdictional element in § 2318(c)(3) for counterfeit or illicit labels that accompany certain classes of works is worded unusually. It allows jurisdiction if the labels were affixed or designed to be affixed to copies of sound recordings, musical works, computer programs, motion pictures, audiovisual works, or documentation and packaging, if those items were "copyrighted." It also allows jurisdiction if the labels were affixed or designed to be affixed to literary works, pictorial, graphic or sculptural works, or works or visual art, but does not indicate that these items must have been "copyrighted." *Compare* § 2318(c)(3)(A)-(C), (G), *with* § 2318(c)(3)(D)-(F). However, these latter classes of works are subject to copyright protection, and § 2318 intends these terms to have the same meaning as in the copyright code. *See* 17 U.S.C. § 102; 18 U.S.C. § 2318(b)(3). Therefore, Congress's omission of the word "copyrighted" from § 2318(c)(3)(D)-(F) was probably unintended, and therefore copyright should be read as necessary to establish jurisdiction under § 2318(c)(3), even for literary, pictorial, or visual art works.

The government need not prove the defendant knew that his actions fell within the federal jurisdiction elements set forth in 18 U.S.C. § 2318(c). Thus, it is unnecessary to prove, for example, that the defendant knew that the copy of the computer program to which his counterfeit labels were affixed was copyrighted (see Section B.1. of this Chapter). *Cf. United States v. Feola*, 420 U.S. 671, 676 n.9 (1975) ("[T]he existence of the fact that confers federal jurisdiction need not be one in the mind of the actor at the time he perpetrates the act made criminal by the federal statute."); *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 72 n.3 (1994) (affirming *Feola* as applied to strictly jurisdictional facts); *United States v. Yermian*, 468 U.S. 63, 68-70 (1984) (holding that the plain language of 18 U.S.C. § 1001, which is worded

similarly to § 2318(a), indicates that Congress did not intend "knowingly and willfully" to apply to jurisdictional element).

6. Venue

The proper venue for a § 2318 prosecution is addressed by general principles governing venue in criminal cases. Particular attention should be paid to offenses that involve the use of the mail or transportation in interstate or foreign commerce, which will occur in most § 2318 offenses.

C. Defenses

1. Statute of Limitations

Because § 2318 does not contain a specific statute of limitations, the general five-year statute of limitations for non-capital offenses applies. *See* 18 U.S.C. § 3282.

2. First Sale (Does Not Apply)

Some defendants have sought to raise a "first sale" defense to a § 2318 charge, particularly a charge involving illicit labels, which, by definition, are genuine items that may have been obtained by the defendant legitimately. Although the "first sale" doctrine provides a valid defense to a charge of copyright infringement (*see* 17 U.S.C. § 109; Chapter II of this Manual, *supra*), permitting a person who has lawfully obtained title to a particular copy of a work to transfer or dispose of that particular copy without authorization from the copyright owner, Congress did not incorporate such a defense into § 2318. Indeed, for Congress to have done so would have eviscerated the purpose of § 2318's illicit labels provision, which is designed to prohibit traffic in genuine labeling components that may be used to facilitate infringement. Courts have rejected attempts to raise a first sale defense in the context of § 2318. *See United States v. Harrison*, 534 F.3d 1371, 1373 (11th Cir. 2008).

D. Special Issues

1. Electronic Copies of Labels, Documentation, or Packaging

Although a typical case under § 2318 generally involves labels, docutmentation, or packaging in some sort of physical form, such as an adhesive decal, a cardboard box, or a manual printed on paper, § 2318 might also be

applied in certain limited circumstances to cases when either the "original" or "legitimate" items, or the "counterfeit" or "illicit" copies, or both, are in electronic or digital form. Section 2318(b)(5) defines documentation and packaging as items which are "in physical form," which would not prohibit trafficking in unauthorized copies of electronic documentation or manuals, when the original or legitimate versions are only available in electronic form, e.g., for download over the Internet. It is unclear whether the term "in physical form" would include a digitally-formatted manual tangibly embodied on a CD-ROM. Conduct involving unauthorized electronic copies of a physical version of a documentation or packaging (such as image files scanned from a paper manual or box), or of documentation that is legitimately distributed on a CD-ROM, nevertheless may implicate § 2318, either as evidence of a substantive violation of the trafficking provision, or as an act that aids or abets such trafficking or furthers a conspiracy to traffic.

The House Report to the 2004 amendments also makes clear that § 2318's criminal provisions do not apply to "electronic transmission" of "genuine" licensing components, documentation, or packaging. *See* H.R. Rep. No. 108-600, at 4 (2004) (stating that the amendments "shall not be construed to apply ... in any case, to the electronic transmission of a genuine certificate, licensing document, registration card, similar labeling component, or documentation or packaging"). This language suggests that the unauthorized electronic distribution of labeling components that are purely electronic in their original or legitimate form, such as electronic signatures or watermarks, does not constitute criminal trafficking under § 2318 (although such conduct may violate other criminal statutes). However, the statute is silent as to whether § 2318 applies to the electronic transmission of labeling components that are *not* "genuine," suggesting that it could be a criminal violation of § 2318 to traffic in electronic files that contain unauthorized copies of labeling components, where the original or legitimate labeling components were in physical form (e.g., trafficking in digital image files that contain a convincing reproduction of label decals or product packaging, such as would be suitable for printing additional counterfeit copies of the labels or packaging). Nevertheless, to date courts have not addressed the extent to which § 2318 may be applied in situations involving purely electronic labeling components.

2. Advantages of Charging a § 2318 Offense

A § 2318 charge may be an appropriate adjunct or alternative charge when the offense involves copyright or trademark infringement. In many cases, the

§ 2318 charge may even be preferable. The mens rea (knowledge) and minimum threshold of illegal conduct (none) are both lower than the mens rea required in criminal copyright charges (willfulness) and the monetary and numerical thresholds for many criminal copyright charges. See Chapter II of this Manual. The standard of proof may also be lower than for criminal trademark charges, which require proof that any trademarks used on the counterfeit or illicit labeling are identical to or substantially indistinguishable from one registered with the U.S. Patent and Trademark Office. See Chapter III of this Manual.

E. Penalties

Section 2318(a) provides for a fine or imprisonment or both. Forfeiture and restitution are also available under § 2318(d).

1. Fines

Under § 2318(a), a defendant may be "fined under this title [18]," which is an indirect reference to 18 U.S.C. § 3571 ("Sentence of fine"). Under 18 U.S.C. § 3571, an individual can be fined up to $250,000 and an organization can be fined up to $500,000, or either can be fined twice the offense's pecuniary gain or loss, without limit. 18 U.S.C. § 3571(a)-(d).

2. Imprisonment

The maximum term of imprisonment is five years. 18 U.S.C. § 2318(a).

3. Restitution

Section 2318(d) specifies that restitution shall be subject to 18 U.S.C. § 2323, the general forfeiture and restitution provision for IP offenses created by the PRO-IP Act. According to Section 2323(c): "[w]hen a person is convicted of an offense under [§ 2318, *inter alia*], the court, pursuant to sections 3556, 3663A, and 3664 of this title, shall order the person to pay restitution to any victim of the offense as an offense against property referred to in section 3663A(c)(1)(A)(ii)." In turn, 18 U.S.C. § 3663A provides for mandatory restitution to victims of certain crimes, including crimes against property in Title 18, of which § 2318 is one. 18 U.S.C. § 3663A(c)(1)(A)(ii). Section 5E1.1 of the U.S. Sentencing Guidelines Manual also provides for restitution in cases where there is an identifiable victim and restitution is authorized under 18 U.S.C. § 3663A. Courts have affirmed restitution orders for convictions under § 2318. *See United States v. Chay*, 281 F.3d 682,

686 (7th Cir. 2002) (holding that an 18 U.S.C. § 2318(a) offense is "a crime against property covered by the Mandatory Victim Restitution Act (MVRA), 18 U.S.C. § 3663A" and affirming an order of $49,941.02 in restitution); *United States v. Elouri*, 62 Fed. Appx. 556 (5th Cir. 2003) (affirming an order on procedural grounds of $136,050 in restitution for a violation of § 2318). For more on restitution, see Chapter VIII of this Manual.

4. Forfeiture

Seizure, forfeiture, and destruction of items in connection with a violation of § 2318 is governed by 18 U.S.C. § 2323. *See* 18 U.S.C. § 2318(d). Section 2323(b) requires a court, in imposing a sentence for violation of § 2318, to order the defendant to forfeit all counterfeit or illicit labels or other items the making or trafficking of which is prohibited under § 2318, as well as any property used or intended to be used in the offense, and any property constituting or derived from proceeds of the offense. Section 2323 also authorizes civil forfeiture of such items, apart from a criminal proceeding. For more on forfeiture, see Chapter VIII of this Manual.

5. Sentencing Guidelines

Section 2B5.3 is the applicable sentencing guideline. See Chapter VIII of this Manual. Under § 2B5.3, often the most significant factor in the calculation of a sentence is the "infringement amount." *See* § 2B5.3(b)(1). In copyright or trademark counterfeiting cases, the infringement amount is generally based on the number of infringing items multiplied by the retail price of either the genuine or infringing item. Because labels and packaging are generally not sold separately through legitimate retail channels, however, § 2318 offenses raise how such items should be valued for purposes of determining the infringement amount, particularly where the labels or packaging at issue have not been affixed to actual copies or goods.

Application Note (2)(A)(vii) addresses valuation in cases under § 2318 involving such "unaffixed" counterfeit or illicit labels (or other items):

> (vii) A case under 18 U.S.C. § 2318 or § 2320 that involves a counterfeit label, patch, sticker, wrapper, badge, emblem, medallion, charm, box, container, can, case, hangtag, documentation, or packaging of any type or nature (I) that has not been affixed to, or does not enclose or accompany a good or service; and (II) which, had it been so used, would appear to

> a reasonably informed purchaser to be affixed to, enclosing or accompanying an identifiable, genuine good or service. In such a case, the "infringed item" is the identifiable, genuine good or service.

§ 2B5.3 n. 2(A)(vii). Thus, in a determining a Guideline sentence in a § 2318 case, if a counterfeit or illicit label has not been affixed to an actual copy of a copyrighted work, but the court finds that the label, if it had been used, would make it appear to a reasonably-informed purchaser that the item to which it was affixed was genuine, then the infringement amount should be determined based on the value of the item to which the item was designed to be affixed, rather than the (generally much lower) value of the label itself.

Application Note 2(A)(vii) was added in 2006 in response to a provision of the Stop Counterfeiting in Manufactured Goods Act, which directed the Sentencing Commission to address how the infringement amount should be calculated for offenses involving labels, documentation, and packaging, that are not attached to or accompanying copyrighted works. *See* Pub. L. No. 109-181, § 1, 120 Stat. 285 (2006).

Prior to the 2006 Guidelines amendments, § 2B5.3 offered little guidance as to how unattached labels or packaging should be valued, leading courts to devise various theories for valuing such items for sentencing purposes. In *United States v. Bao*, 189 F.3d 860, 862-63 (9th Cir. 1999), the government seized 5,000 counterfeit manuals for software and counterfeit packaging materials such as CD-ROM inserts and product registration cards in Bao's print shop. After Bao's conviction under § 2318 for trafficking in counterfeit software manuals, the district court sentenced him based on a retail value of $50 per manual, the black market value of the software plus a manual. The court's theory was that the manual had no value apart from the software. *Id.* at 862-63, 867. The Ninth Circuit vacated the sentence, holding that the manuals' retail value should have been $12 apiece, the retail value of other comparable genuine manuals the victim sold separate from software. *Id.* at 866-67. In other words, the appropriate retail value was that of the counterfeit documentation, not the thing the documentation was to accompany. *Cf. U.S. v. Guerra*, 293 F.3d 1279, 1292 (11th Cir. 2002) (§ 2320 case holding that "[t]he value of the bands and labels is inextricably intertwined with that of the completed product, as the value of the counterfeit cigars derives primarily from the degree to which the bands and labels bear marks that are indistinguishable

from the genuine marks. Thus, the district court did not err by considering 'infringing items' to be cigars rather than labels.").

Just as the retail value might depend on how many products the defendant had completed or could have completed readily, so might the *number* of infringing items. Two appellate courts have ruled that "the number of infringing items should correspond to the number of completed or nearly completed counterfeit goods." *U.S. v. Guerra*, 293 F.3d 1279, 1293 (11th Cir. 2002) (citing *United States v. Sung*, 51 F.3d 92, 94-96 (7th Cir. 1995), *appeal after remand*, 87 F.3d 194 (7th Cir. 1996), *on remand to*, 940 F. Supp. 172 (N.D. Ill. 1996), *rev'g trial court on other grounds*, 114 F.3d 1192 (1997)). In both these cases, the number of infringing items was held to be not the number of infringing labels or packaging items, but rather the lower number of goods to which the labels or packaging had been or could readily have been attached. *See id*.

However, both these cases concerned sentencing under a previous version of the counterfeit trademark criminal statute, 18 U.S.C. § 2320, which did not expressly apply to unattached labels or packaging, as both § 2318 and the current version of § 2320 now do. Under § 2318 (as well as § 2320), trafficking in counterfeit labels is not treated as an attempt to traffic in goods to which the labels might be affixed, but as a separate and complete offense, and therefore, a defendant's sentence may properly be calculated based on the number of labels involved, rather than only on those labels that have already been affixed to an actual product. Further, Application Note 2(A)(vii) provides that in determining the infringement amount in § 2318 cases involving labels that, if used, would lead a reasonable purchaser to believe the items to which the labels were attached were genuine, the "infringed item" is the item to which the labels would be attached. Therefore, in such cases, the infringement amount should be based on the retail value of such item, multiplied by the number of labels.

F. Other Charges to Consider

When confronted with a case that implicates counterfeit or illicit labels or counterfeit documentation or packaging, prosecutors may want to consider the following crimes for charges in addition to 18 U.S.C. § 2318 or in lieu of such charges if § 2318's elements cannot be met:

- **Copyright infringement, 17 U.S.C. § 506, 18 U.S.C. § 2319,** for any infringement of the underlying copyrighted goods. *See, e.g., United*

States v. Cohen, 946 F.2d 430, 433-34 (6th Cir. 1991) (affirming conviction under 18 U.S.C. §§ 2318-2319 for duplicating and distributing copyrighted movies). A conspiracy or aiding-and-abetting theory will sometimes be necessary. See Chapter II of this Manual.

- **Trademark counterfeiting, 18 U.S.C. § 2320,** because labels, documentation, and packaging for copyrighted works often carry counterfeit reproductions of federally registered trademarks. *See, e.g., United States v. Beltran*, 503 F.3d 1, 2-4 (1st Cir. 2007) (upholding convictions under 18 U.S.C. §§ 2318-2320 for counterfeit DVDs and VHS tapes); *United States v. Hernandez*, 952 F.2d 1110, 1113-14 (9th Cir. 1991) (affirming conviction under 18 U.S.C. §§ 2318-2320 for counterfeit audio cassettes and audio cassette labels). See Chapter III of this Manual.
- **Mail or wire fraud, 18 U.S.C. §§ 1341, 1343,** for schemes that involve the use of the mails or wire, as long as there is a scheme to defraud. *Cf. United States v. Shultz*, 482 F.2d 1179, 1180 (6th Cir. 1973) (upholding convictions for mail fraud and counterfeit labels under an earlier version of § 2318, for causing the transportation of a counterfeit stereo tape cartridge recording in interstate commerce with forged or counterfeit label). The theory of fraud cannot be merely that the media was copyrighted, but rather that the defendant must have intended to defraud either his immediate purchaser or other downstream purchasers. See Chapter II, Section F. of this Manual.
- **Racketeer Influenced and Corrupt Organizations (RICO), 18 U.S.C. §§ 1961-1968,** because § 2318 violations serve as RICO predicate acts. *See* § 1961(1)(B). RICO charges must be approved by the Department's Organized Crime and Gang Section, which can be reached at (202) 514-3594.
- **Bootleg sound recordings and music videos of live musical performances, 18 U.S.C. § 2319A.** See Chapter II, Section F. of this Manual.

VII. Patent

A. Overview of Patent

Unlike copyright and trademark infringement, there are no criminal penalties for committing patent infringement. *Dowling v. United States*, 473 U.S. 207, 227 (1985) (noting that "[d]espite its undoubted power to do so," Congress has not provided criminal penalties for patent infringement). Congress instead has relied on provisions affording owners a civil cause of action for patent infringement. *Id.* at 227 n.19. As set forth more fully below, however, Congress has provided for two criminal provisions relating to patents: forgery of letters patent, and false marking of patents.

As a threshold matter, it is worth revisiting the differences between patents and copyrights. Patent rights are available to anyone who invents "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." 35 U.S.C. § 101. A patent grants an inventor the right to exclude others from making, using, offering for sale, or selling devices that embody the patented invention. *See* 35 U.S.C. § 271(a); *Eldred v. Ashcroft*, 537 U.S. 190, 216 (2003) (citing *Sears, Roebuck & Co. v. Stiffel Co.*, 376 U.S. 225, 229 (1964)). The federal government's authority to grant patents stems from Article I, Section 8, Clause 8 of the U.S. Constitution, known as the "Intellectual Property" or "Copyright and Patent" Clause, which authorizes Congress to enact statutes that "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." Congress first exercised this authority to grant patents in 1790, when Congress empowered the federal government to issue letters patent. Act of Apr. 10, 1790, ch. 7, § 1, 1 Stat. 109 (1790). Like their modern counterparts, "letters patent" contain a short title of the invention and a "grant" to the patent owner ("patentee"), and his or her heirs or assigns, of the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States. *Cf. Eldred*, 537 U.S. at 216; 35 U.S.C. § 154(a)(1). Currently, a patent grant lasts for a term beginning on the date the U.S. Patent and Trademark Office issues the patent and ending

20 years from the date on which the patentee filed his or her application for a patent grant. 35 U.S.C. § 154(a)(2).

Although patents and copyrights share a common constitutional source (and the concomitant requirement that these exclusive rights are for "limited Times"), they differ in several meaningful respects. First, copyrights grant an author the right to exclude certain uses of the author's expression of an idea contained in an "original work of authorship," whereas patents grant an author the right to exclude others from making, using, and selling devices or processes that embody the claimed invention. *See* 17 U.S.C. § 102(a); 35 U.S.C. § 154(a)(1). Second, in exchange for granting the patentee this right to exclude, the patentee must publicly disclose the invention. *Eldred*, 537 U.S. at 216. "For the author seeking copyright protection, in contrast, disclosure is the desired objective, not something exacted from the author in exchange for the copyright." *Id.* Third, a copyright gives the holder no monopoly on any knowledge or idea; a reader of an author's writing may make full use of any fact or idea acquired by reading the writing. *See* 17 U.S.C. § 102(b); *Eldred*, 537 U.S. at 217. A patent, on the other hand, gives the patentee a monopoly on his invention to prevent the full use by others of the knowledge embodied in the patent. *See Eldred*, 537 U.S. at 217.

It is also worth considering the difference between a patent and a trade secret. The first difference is naturally that trade secret information is protected only if it is secret (see Chapter IV, Section B.3.a.ii. of this Manual), whereas a patent is protected even after disclosure. During the patent process, a trade secret contained in a patent application may lose its trade secret protection through disclosure only to gain patent protection. (See Chapter IV, Section C.1.b.ii. of this Manual.) Second, a patent gives its owner an exclusive right to his invention, even against another who discovered the patented invention independently, whereas a trade secret, like a copyright, gives its owner no protection against independent discovery. *ConFold Pac., Inc. v. Polaris Indus.*, 433 F.3d 952, 958-59 (7th Cir. 2006) (Posner, J.).

B. Forgery of Letters Patent—18 U.S.C. § 497

Forging "letters patent" (described above) and knowingly passing off counterfeit letters patent are prohibited by 18 U.S.C. § 497:

> Whoever falsely makes, forges, counterfeits, or alters any letters patent granted or purporting to have been granted by

> the President of the United States; or Whoever passes, utters, or publishes, or attempts to pass, utter, or publish as genuine, any such letters patent, knowing the same to be forged, counterfeited or falsely altered—Shall be fined under this title or imprisoned not more than ten years, or both.

As of this writing, no published opinions reported an applicable offense under this provision, although one court noted that Congress enacted the statute to "criminalize[] activities likely to impugn the reputation or integrity of the federal government regardless of whether the perpetrator intended to defraud private citizens." *United States v. Reich*, 479 F.3d 179, 189 (2d Cir. 2007). The statute is one of many "designed to protect the integrity of government functions" but "do[es] not include the intent to defraud as an element of the crime of forgery." *United States v. Cowan*, 116 F.3d 1360, 1363 (10th Cir. 1997).

C. False Marking of Patent—35 U.S.C. § 292

To protect patent holders and the public, Congress enacted the false marking provision, 35 U.S.C. § 292, which provides for both criminal and civil actions against a defendant for false marking. Section 292(a) creates a financial punishment for three types of improper marking: (1) representing that an article is patented when the patent is in fact held by another; (2) marking as patented an article that is not patented; and (3) falsely claiming that a patent application has been made or is pending. In 2011, the statute's scope was narrowed pursuant to the Leahy-Smith America Invents Act so that it is no longer a violation of the statute where "[t]he marking of a product ... with matter relating to a patent that covered that product but has expired." 35 U.S.C. § 292(c). Section 16(b)(4) of the Act makes this and its other amendments to the false marking statute applicable "to all cases, without exception, that are pending on, or commenced on or after, the date of the enactment of this Act," on September 16, 2011. Leahy-Smith America Invents Act, Pub. L. No. 112-29, § 16(b)(4), 125 Stat. 284, 329 (2011).

Congress prohibits false marking in part because a properly marked patented article provides the public with "a ready means of discerning the status of the intellectual property embodied in an article of manufacture or design." *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 162 (1989). This is consistent with federal patent policy, which recognizes an "important public

interest in permitting full and free competition in the use of ideas which are in reality a part of the public domain." *Lear, Inc. v. Adkins*, 395 U.S. 653, 670 (1969). "Acts of false marking deter innovation and stifle competition in the marketplace." *Forest Group, Inc. v. Bon Tool Co.*, 590 F.3d 1295, 1302 (Fed. Cir. 2009). False marking harms that public interest because it "misleads the public into believing that a patentee controls the article in question (as well as like articles), externalizes the risk of error in the determination, placing it on the public rather than the manufacturer or seller of the article, and increases the cost to the public of ascertaining whether a patentee in fact controls the intellectual property embodied in an article." *Clontech Labs., Inc. v. Invitrogen Corp.*, 406 F.3d 1347, 1356-57 (Fed. Cir. 2005) (footnote omitted); *see also Calderwood v. Mansfield*, 71 F. Supp. 480, 482 (N.D. Cal. 1947) (noting that, under § 50, the former version of § 292, one purpose of the "false marking" statute was to "penalize those who would palm off upon the public unpatented articles, by falsely and fraudulently representing them to have been patented").

Section 292(a)'s first prohibition protects patent holders by prohibiting an individual, without a patent holder's consent, from marking or using in advertising for a product:

> the words "patent," "patentee," or the like, with the intent of counterfeiting or imitating the mark of the patentee, or of deceiving the public and inducing them to believe that the thing was made, offered for sale, sold, or imported into the United States by or with the consent of the patentee.

35 U.S.C. § 292(a).

Section 292(a)'s second and third paragraphs protect the public from false or misleading patent claims. The second paragraph prohibits individuals from marking or using in advertising the word "patent" in connection with any "unpatented article" for the purpose of deceiving the public. *Clontech*, 406 F.3d at 1352. For § 292 to apply, the mismarked article must "actually exist" and "be completed." *Lang v. Pac. Marine & Supply Co.,* 895 F.2d 761, 765 (Fed. Cir. 1990).

Although not defined in the statute, an "unpatented article" is one that is not covered by any claim of any of the patents marked on the article. Or, as the Federal Circuit has held, an "unpatented article" means that "the article in question is not covered by at least one claim of *each* patent with which the article is marked. Thus, in order to determine if an article is 'unpatented' for

purposes of section 292, it must be first determined whether the claims of a patent cover the article in question." *Clontech*, 406 F.3d at 1352 (emphasis added). Although earlier courts consistently had found no violation of § 292 "by a patentee who marks patented articles with more patents than actually cover the item," *Genlyte Thomas Grp. LLC v. National Serv. Indus., Inc.*, 262 F. Supp. 2d 753, 756 (W.D. Ky. 2003) (internal citations and quotations omitted), the Federal Circuit's decision in *Clontech* appears to have foreclosed this interpretation of an "unpatented article." *Brinkmeier v. Graco Children's Products Inc.*, 684 F. Supp. 2d 548, 551 (D. Del. 2010) ("The court rejects Defendant's contention that no actionable mismarking can occur if the product at issue is covered by at least one claim of the patents listed."); *DP Wagner Mfg. Inc. v. Pro Patch Sys., Inc.*, 434 F. Supp. 2d 445, 455 (S.D. Tex. 2006) (holding that the Federal Circuit's construction of "unpatented article" is controlling, "notwithstanding the fact that other courts may have interpreted the term differently in the past").

Prior to the 2011 passage of the Leahy-Smith America Invents Act, the Federal Circuit had held that "an article covered by a now-expired patent is 'unpatented.'" *Pequignot v. Solo Cup Co.*, 608 F.3d 1356, 1361 (Fed. Cir. 2010); *see also Bonito Boats*, 489 U.S. at 159 (An article that "has been freely exposed to the public ... stands in the same stead as an item for which a patent has expired or been denied: it is unpatented and unpatentable"). "Thus, as with a never-patented article, an article marked with an expired patent number imposes on the public 'the cost of determining whether the involved patents are valid and enforceable.'" *Pequignot*, 608 F.3d at 1362 (quoting *Clontech*, 406 F.3d at 1357 n.6). However, as already noted, the Act amended the false marking statute so that this conduct no longer constitutes a violation of § 292(a). 35 U.S.C. § 292(c).

Notably, "the *omission* of 'applicable patents' from a label listing patents purporting to cover the contents of a box of course cannot, in itself, be a violation of the *false* marking statute." *Arcadia Mach. & Tool, Inc. v. Sturm, Ruger & Co.*, 786 F.2d 1124, 1125 (Fed. Cir. 1986) (emphasis in original).

In the same vein as § 292(a)'s second paragraph, the third paragraph prohibits individuals from marking or using in advertising the words "patent applied for" or "patent pending" for the purpose of deceiving the public when a patent application has neither been made nor is pending. 35 U.S.C. § 292(a).

Section 292(a) imposes a fine of not more than $500 for every offense. 35 U.S.C. § 292(a). Thus, "the statute's plain language requires the penalty to be imposed on a per article basis," not on a "per decision" nor a "time-based approach." *Forest Group*, 590 F.3d at 1301-04 (reversing district court's holding that penalty be imposed for each "decision" to mark multiple articles falsely). "Section 292 clearly requires a per article fine." *Id.* at 1302. The "per article" unit of prosecution is consistent with the purpose behind the statute because "[t]he more articles that are falsely marked[,] the greater the chance that competitors will see the falsely marked article and be deterred from competing." *Id.* at 1303.

Significantly, the statute was amended in 1952 to remove any minimum fine. *Id.* at 1302. Thus, "district courts have the discretion to assess the per article fine at any amount up to $500 per article." *Id.* Courts, for example, have the discretion to impose a penalty of a fraction of a penny per article. *Id.* at 1304. As a result, courts may use their "discretion to strike a balance between encouraging enforcement of an important public policy and imposing disproportionately large penalties for small, inexpensive items produced in large quantities." *Id.* Because the fine for an infraction of 35 U.S.C. § 292 is a criminal fine, that fine is increased by 18 U.S.C. § 3571 to a maximum of $5,000 for individuals ($10,000 for corporations) or twice the monetary gain or loss. *See* 18 U.S.C. § 3571(b)(2), (b)(7), (c)(2), (c)(7), (d).

Prior to the Leahy-Smith America Invents Act, § 292(b) provided for a civil qui tam remedy, which enabled any person to sue for the statutory penalty set forth in § 292(a) and retain one-half of the recovery, leaving the other half "to the use of the United States." 35 U.S.C. § 292(b) (2010); *Boyd v. Schildkraut Giftware Corp.*, 936 F.2d 76, 79 (2d Cir. 1991); *Filmon Process Corp. v. Spell-Right Corp.*, 404 F.2d 1351, 1355 (D.C. Cir. 1968) (holding that "§ 292(b), while penal, is not a criminal statute"). "The patentee is given this remedy to protect his patent position, and as a practical matter, the patentee is the only likely enforcer of it, as recovery requires proof that the statements were made without his consent." *Filmon*, 404 F.2d at 1355.

The Leahy-Smith America Invents Act made two substantive changes impacting the predecessor statute's *qui tam* remedy. First, it eliminated the *qui tam* action. The Act added to section 292(a) that "[o]nly the United States may sue for the penalty authorized by this subsection," and removed the qui tam action from section 292(b). America Invents Act § 16(b)(1) & (2). Second, the Act replaced the *qui tam* remedy with a civil compensatory damages action: "A

person who has suffered a competitive injury as a result of a violation of this section may file a civil action in a district court of the United States for recovery of damages adequate to compensate for the injury." 35 U.S.C. § 292(b).

However, because criminal prosecutions pursuant to § 292 are rare, reported *qui tam* actions under the predecessor version of the false marking law are still helpful authority for interpreting the false marking statute in criminal cases. For example, at least one court rejected a private enforcement pursuant to § 292(b) because, *inter alia*, "the patent markings about which Plaintiffs complain were found on the packaging, and not on the product." *Rainworks Ltd. v. Mill-Rose Co.*, 609 F. Supp. 2d 732, 739 (N.D. Ohio 2009) (holding that "[b]ecause marking the outer packaging, when marking the product could be done, is insufficient for the notice requirements of 35 U.S.C. § 287(a), the actions of Defendants ... are equally insufficient for false marking liability under the penal statute, 35 U.S.C. § 292(a)"). In other words, if the marking is insufficient to meet patent law's notice requirement, then the marking is also insufficient to support a claim under false marking statute.

Consistent with the express language of the statute, courts have held that 35 U.S.C. § 292(a) requires the government to prove that the defendant intended to deceive or counterfeit. *See Arcadia*, 786 F.2d at 1125 (affirming holding that false marking statute was not violated where there was no evidence of intent to deceive). Thus, accidental or unintentional mismarking is not a violation. *London v. Everett H. Dunbar Corp.*, 179 F. 506, 510 (1st Cir. 1910) (holding that interpreting patent claims is not an exact science, and hence where one "has an honest, though mistaken, belief that upon a proper construction of the patent it covers the article which he marks," the requisite intent to deceive would not be shown); *Brose v. Sears, Roebuck & Co.*, 455 F.2d 763, 768-69 (5th Cir. 1972) (same).

"Intent to deceive is a state of mind arising when a party acts with sufficient knowledge that what it is saying is not so and consequently that the recipient of its saying will be misled into thinking that the statement is true." *Clontech*, 406 F.3d at 1352 (citing *Seven Cases v. United States*, 239 U.S. 510, 517-18 (1916)). Using "objective standards," the prosecution may establish a rebuttable presumption of the requisite intent to deceive where the government proves both (1) the fact of misrepresentation and that (2) the party making it had knowledge of its falsity. *See id.* (citing *Norton v. Curtiss*, 433 F.2d 779, 795-96 (C.C.P.A. 1970)); *Pequignot*, 608 F.3d at 1362-63 ("the combination of a false statement and knowledge that the statement was false creates a rebuttable

presumption of intent to deceive the public, rather than irrebuttably proving such an intent"). A defendant's "mere assertion" that he did not intend to deceive will not allow him to rebut the presumption. *Pequignot*, 608 F.3d at 1363; *Clontech*, 406 F.3d at 1352, 1353 n.2 (noting that "the inference of intent to deceive cannot be defeated with blind assertions of good faith where the patentee has knowledge of mismarking"). By the same token, "mere knowledge that a marking is false is insufficient to prove intent if [the defendant] can prove that it did not consciously desire the result that the public be deceived." *Pequignot*, 608 F.3d at 1363. "Thus, a good faith belief that an action is appropriate ... can negate the inference of a purpose of deceiving the public." *Id.* at 1364 (holding that advice of counsel and purpose other than deceiving the public sufficient to rebut presumption of intent to deceive).

In addition, "[w]here the article marked is obviously very remote from the patent referred to in justification of the marking, this difference alone may be sufficient to show an intention to deceive; but where the difference is slight, and the question of the breadth of the invention or of the claims is so close as to permit of an honest difference of opinion," then proof of such intent is more difficult. *London*, 179 F. at 510. Hence, to show knowledge of the misrepresentation, the government must show beyond a reasonable doubt that the articles in question were in fact mismarked, and that defendant did not have a reasonable belief that the articles were properly marked (i.e., covered by a patent or patent application). *Cf. Clontech*, 406 F.3d at 1352-53.

D. No Prosecution for Interstate Transportation or Receipt of Stolen Property—18 U.S.C. §§ 2314, 2315

The interstate transportation of stolen property statute, 18 U.S.C. § 2314, does not allow prosecution of a person for the interstate distribution of patent-infringing goods when the only theory for the property's being stolen is that it infringes a patent. *See Dowling v. United States*, 473 U.S. 207, 227 (1985) (dicta). The same dicta would likely apply to the interstate receipt of stolen property (18 U.S.C. § 2315).

VIII. Penalties, Restitution, and Forfeiture

A. Introduction

This Chapter discusses the penalties for intellectual property crime, concentrating on the statutory sentencing factors, the United States Sentencing Guidelines (the "Guidelines"), restitution, and forfeiture.

The Supreme Court's seminal decision in *United States v. Booker*, 543 U.S. 220 (2005), changed the landscape of federal criminal sentencing. In *Booker*, the Supreme Court held that mandatory application of the Guidelines violated the Sixth Amendment right to trial by jury. Accordingly, the Supreme Court made the Guidelines advisory and excised the statutory provision which allowed departures only under certain very limited circumstances. *See* 18 U.S.C. § 3553(b)(1).

The Guidelines still occupy a central role in sentencing, but are now just one of several statutory factors courts must consider. *See* 18 U.S.C. § 3553(a). Generally, sentencing courts will first consult the Guidelines, which will normally include calculating an advisory range of imprisonment. *See Booker*, 543 U.S. at 264; *Gall v. United States*, 552 U.S. 38, 46 (2007); *Rita v. United States*, 551 U.S. 338, 347-48 (2007); *see also United States v. Crosby*, 397 F.3d 103, 111 (2d Cir. 2005) ("[T]he excision of the mandatory aspect of the Guidelines does not mean that the Guidelines have been discarded. On the contrary, sentencing judges remain under a duty with respect to the Guidelines--not the previously imposed duty to apply the Guidelines, but the continuing duty to 'consider' them, along with the other factors listed in section 3553(a)."). The Guidelines are not entitled to greater weight than the other § 3553(a) factors. *See Gall*, 552 U.S. at 51 (deferential abuse-of-discretion standard applies to sentencing decisions both inside and outside of Guidelines range). After a Guideline determination is made, sentencing courts then consider all of § 3553(a) factors. *See id*. at 50.

Appellate courts now review federal sentences for "reasonableness." *Booker*, 543 U.S. at 260-61. This is both a procedural and a substantive inquiry. A

sentence may be unreasonable if the sentencing court commits procedural error by, among other things, failing to consider all of the factors in § 3553(a), or treating the Guidelines as mandatory. *Gall* at 51. Substantive reasonableness is based on the totality of the circumstances, including any variance from the Guidelines range. *Id.* But while a sentencing court may presume that a Guidelines sentence is reasonable, *see Rita*, 551 U.S. at 347, a non-Guidelines sentence based upon consideration of all of the § 3553 factors may also be reasonable. *See Gall*, 552 U.S. at 51 (reviewing courts "must give due deference to the district court's decision that the § 3553(a) factors, on a whole, justify the extent of the variance").

B. The Statutory Sentencing Factors

This subsection discusses how courts have used the following § 3553(a) sentencing factors in intellectual property cases:

> (a) Factors to be considered in imposing a sentence.--The court shall impose a sentence sufficient, but not greater than necessary, to comply with the purposes set forth in paragraph (2) of this subsection. The court, in determining the particular sentence to be imposed, shall consider--
>
> (1) the nature and circumstances of the offense and the history and characteristics of the defendant;
>
> (2) the need for the sentence imposed--
>
> (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
>
> (B) to afford adequate deterrence to criminal conduct;
>
> (C) to protect the public from further crimes of the defendant; and
>
> (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner;
>
> (3) the kinds of sentences available;

(4) the kinds of sentence and the sentencing range established for--

(A) the applicable category of offense committed by the applicable category of defendant as set forth in the guidelines--

(i) issued by the Sentencing Commission pursuant to section 994(a)(1) of title 28, United States Code, subject to any amendments made to such guidelines by act of Congress (regardless of whether such amendments have yet to be incorporated by the Sentencing Commission into amendments issued under section 994(p) of title 28); and

(ii) that, except as provided in section 3742(g), are in effect on the date the defendant is sentenced; or

(B) in the case of a violation of probation or supervised release, the applicable guidelines or policy statements issued by the Sentencing Commission pursuant to section 994(a)(3) of title 28, United States Code, taking into account any amendments made to such guidelines or policy statements by act of Congress (regardless of whether such amendments have yet to be incorporated by the Sentencing Commission into amendments issued under section 994(p) of title 28);

(5) any pertinent policy statement--

(A) issued by the Sentencing Commission pursuant to section 994(a)(2) of title 28, United States Code, subject to any amendments made to such policy statement by act of Congress (regardless of whether such amendments have yet to be incorporated by the Sentencing Commission into amendments issued under section 994(p) of title 28); and

(B) that, except as provided in section 3742(g), is in effect on the date the defendant is sentenced.

(6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and

(7) the need to provide restitution to any victims of the offense.

18 U.S.C. § 3553(a). While courts need not engage in "robotic incantation" of the § 3553(a) factors, *see Crosby*, 397 F.3d at 113, *Booker* and its progeny have spurred sentencing courts to emphasize and articulate their reliance on these statutory factors, notwithstanding the applicable Guidelines range.

This is clearly evident in intellectual property cases. Sentencing courts have used the § 3553(a) factors to justify sentences above the Guidelines range. *See United States v. Williams*, 526 F.3d 1312, 1322-23 (11th Cir. 2008) (in trade secret case, affirming sentence above the Guidelines range considering § 3553(a) factors, including: (i) that the defendant lied to the court about her criminal history; (ii) that the defendant was well-educated and did not require vocational education; (iii) the need to protect trade secrets; and (iv) the tremendous harm to the victim had the defendant succeeded); *United States v. Bailey*, 286 Fed. Appx. 678, 682 (11th Cir. 2008) (in copyright infringement case, sentencing court relied on § 3553(a) evaluation to sentence above the Guidelines range where defendant violated supervised release conditions, highlighting a need for deterrence in light of the defendant's three consecutive release violations); *United States v. Sow*, 180 Fed. Appx. 278, 278-79 (2d Cir. 2006) (in affirming sentence, noting "the District Court found that 'it is clearly Congress' policy decision to treat seriously and punish with significant sentences these sorts of intellectual property and music pirating offenses,' which relates directly to the 'seriousness of the offense.' *See* 18 U.S.C. § 3553(a)(2)(A).").

Courts also have used § 3553(a) analysis to support Guidelines sentences, including when defendants have complained that a correctly calculated Guidelines range is itself unfair. *See United States v. Thomas*, 331 Fed. Appx. 263, 265 (4th Cir. 2009) (in trademark counterfeiting case, affirming Guidelines sentence supported by § 3553(a) evaluation that considered defendant's "lengthy involvement in counterfeit trafficking, his decision to involve his family members in the illegal activity and the scale of his operations," and also distinguished defendant's case from that of his co-conspirators who received

lighter sentences); *United States v. Four Pillars Enter. Co.*, 253 Fed. Appx. 502, 513 (6th Cir. 2007) (affirming Guidelines sentence meted out by district court considering § 3553(a) factors, including: (i) victim impact statements; (ii) the ongoing nature of the scheme; (iii) the defendants' ability to pay a fine; and (iv) the defendants' use of the trade secret owner's own employee for economic espionage); *United States v. Lozano*, 490 F.3d 1317, 1324-25 (11th Cir. 2007) (in trademark counterfeiting case, affirming a Guidelines sentence supported by § 3553(a) factors and further finding that even if the Guidelines calculation were erroneous, the sentence would still have been reasonable based on the § 3553(a) factors, especially the seriousness of the offense—a five-year counterfeiting operation that resulted in at least ten seized shipments of counterfeit cell phone parts; continued even after the defendants knew they were under investigation; and was international, stretching from China to Central America); *United States v. Sagendorf*, 445 F.3d 515, 518 (1st Cir. 2006) (affirming a Guidelines sentence where the district court rejected defendant's contention that the Guidelines range was unfairly high, citing as part of a § 3553(a) the seriousness of the offense and the need for *general* deterrence, even though specific deterrence might have required less).

Finally, courts have used § 3553(a) factors to support sentences below the Guidelines range. *See United States v. Jiang*, No. 09-CR-34, 2009 WL 3254434, at *2 (E.D.N.Y. October 9, 2009) (in trademark counterfeiting case, imposing 30-month sentence, substantially below the 70-87 month Guidelines range, citing § 3553(a) factors, including defendant's "strong work history and many friends and supporters in the community," the adequacy of the sentence to achieve both "general" and "specific" deterrence, the defendant's limited employment prospects and his remorse, even while acknowledging that such violations "destroy American commerce"); *United States v. Kim*, No. 07-0170-S-BLW, 2008 U.S. Dist. LEXIS 80043, at *6-7 (D. Idaho May 8, 2008) (in trademark counterfeiting case, imposing a 1-month sentence, below the 10-16 month Guidelines range, because of § 3553(a) factors, including the nature of offense—the sale of t-shirts in a remote location at prices far below those of genuine goods—and the history and characteristics of the defendant —55, married with five children, all U.S. citizens, with no criminal history and unlikely to reoffend, and facing deportation were a longer sentence imposed); *United States v. Arman*, No. 04-C-6617, 2006 U.S. Dist. LEXIS 4592, at *3-6 (N.D. Ill. February 2, 2006) (in trademark counterfeiting case, imposing sentence substantially below the Guidelines range based on consideration of § 3553(a) factors: (i) no health and safety concerns—defendant sold counterfeit

cameras; (ii) trademark owner not harmed because counterfeits were obviously not genuine; and (iii) no apparent link to organized crime).

The common theme from these cases is that sentencing courts now ignore or trivialize the § 3553(a) factors at their peril. *See Gall*, 552 U.S. at 50-51; *United States v. Kononchuk*, 485 F.3d 199, 204-06 (3rd Cir. 2007) (in trademark counterfeiting case, remanding for resentencing because district court merely gave "rote statement" of § 3553(a) factors in imposing probationary sentence substantially below the Guidelines range, while declining to address any of the government's "cogent" objections, including (i) the disparity in treatment with co-conspirator who was far less culpable and also cooperated fully, but also received a sentence of probation, (ii) the sophistication of the defendant's scheme, and (iii) the inappropriateness of the court's offer to impose probation if the defendant, who had wealthy in-laws, would pay restitution on an accelerated schedule).

C. Sentencing Guidelines

This subsection addresses the interpretation and application of the United States Sentencing Guidelines (U.S.S.G.) in intellectual property prosecutions, primarily § 2B1.1 for Economic Espionage Act cases, § 2B5.3 for all other intellectual property offenses, and § 3B1.3 for crimes in which the defendant abused a position of trust or used a special skill. This subsection should be read in conjunction with the sections covering penalties in the chapters that present the substantive offenses, as well as with the chapter on victims' rights.

As with other crimes, prosecutors should generally continue to seek sentences within the Guidelines range in intellectual property prosecutions. The intellectual property Guidelines have been intricately fashioned through amendment and re-amendment, often incorporating and reacting to court decisions. For general guidance on this issue, prosecutors should consult Attorney General Eric Holder's Memorandum on Department Policy on Charging and Sentencing (May 19, 2010), *available at* http://www.justice.gov/oip/holder-memo-charging-sentencing.pdf, which supersedes all prior memoranda, as well as USAM 9-27.710-760.

For assistance with any sentencing issues specific to intellectual property crimes, please call CCIPS at (202) 514-1026 for assistance.

1. Offenses Involving Copyright (Including Bootleg Music, Camcorded Movies, and the Unauthorized Use of Satellite, Radio, and Cable Communications), Trademark, Counterfeit Labeling, and the DMCA

a. Applicable Guideline is § 2B5.3

Sentencing calculations for the following offenses are governed by U.S.S.G. § 2B5.3:

- Criminal copyright infringement, 17 U.S.C. § 506, 18 U.S.C. § 2319
- Criminal violations of the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 1204
- Trafficking in counterfeit labels, illicit labels, and counterfeit documentation or packaging, 18 U.S.C. § 2318
- Trafficking bootleg audio and video recordings of live musical performances, 18 U.S.C. § 2319A
- Unauthorized recording of motion pictures in a movie theater, 18 U.S.C. § 2319B
- Trafficking in counterfeit trademarked, service-marked, or certification-marked goods, services, and labels, documentation, and packaging for goods and services, 18 U.S.C. § 2320
- Unauthorized reception of cable and satellite service, 47 U.S.C. §§ 553(b)(2), 605 and 18 U.S.C. § 2511

The Guidelines' Statutory Index, U.S.S.G. App. A, refers these statutes to U.S.S.G. § 2B5.3.

Section 2B5.3 has been amended a number of times over the last decade. For example, on May 1, 2000, it was amended to "ensure that the applicable guideline range for a defendant convicted of a crime against intellectual property" would be "sufficiently stringent to deter such a crime and to adequately reflect" consideration of "the retail value and quantity of the items with respect to which the crime against intellectual property was committed." No Electronic Theft (NET) Act of 1997, Pub. L. No. 105-147, § 2(g), 111 Stat. 2678 (1997). Among other things, the May 2000 amendments increased the applicable base offense level from 6 to 8 and increased the number and type of special offense characteristics to include not only the infringement amount, but also characteristics for manufacturing, uploading, or importing infringing items; for infringement not committed for commercial advantage or private financial gain; and for risk of serious bodily injury or possession of a dangerous

weapon in connection with the offense. *See* U.S.S.G. App. C (Amendments 590, 593).

On October 24, 2005, § 2B5.3 was amended under emergency amendment authority, pursuant to the Family Entertainment and Copyright Act of 2005, which: (i) created a new intellectual property offense, "Unauthorized recording of Motion pictures in a Motion picture exhibition facility," codified at 18 U.S.C. § 2319B; and (ii) directed the United States Sentencing Commission (the "Commission") to "review and, if appropriate, amend the Federal sentencing guidelines and policy statements applicable to persons convicted of intellectual property rights crimes ...." Family Entertainment and Copyright Act of 2005, Pub. L. No. 109-9, §§ 102(a), 105(a), 119 Stat. 218, 218-220, 222-23 (2005). Among other things, the October 2005 amendment: (i) added a new specific offense characteristic (2) addressing infringement of pre-release works; (ii) renumbered offense characteristics (2)-(4) as offense characteristics (3)-(5); (iii) clarified the definition of uploading for technical purposes; (iv) clarified that the court can estimate the infringement amount using any relevant information; and (v) provided a reference in the Guidelines' statutory index, Appendix A, assigning the new camcording offense, 18 U.S.C. § 2319B, to § 2B5.3. See U.S.S.G. App. C (Amendment 675). On November 1, 2006, the amendment was repromulgated as permanent, with slight changes to the definition of uploading contained in the original. *See* U.S.S.G. App. C (Amendment 687).

On September 12, 2006, § 2B5.3 was amended again under emergency amendment authority, pursuant to the Stop Counterfeiting in Manufactured Goods Act, which directed the Commission to consider items, such as counterfeit labels and DMCA circumvention devices, that merely facilitate infringement. *See* Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1, 120 Stat. 285, 287-88 (Mar. 16, 2006). The September 2006 amendment provided that in cases under 18 U.S.C. § 2318 or § 2320 involving counterfeit labels, the infringement amount is based on the retail value of the infringed items to which the labels would have been affixed. *See* U.S.S.G. App. C (Amendment 682). On November 1, 2007, the amendment was repromulgated as permanent, adding a provision addressing downward departures for overstated infringement amounts, and several provisions concerning DMCA violations: (i) making § 2B5.3 the applicable guideline; (ii) clarifying that the infringement amount is the retail value of the work accessed; (iii) adding a 2-level enhancement under § 2B5.3; and (iv) making the application of the special skill adjustment under § 3B1.3 discretionary.

See U.S.S.G. App. C (Amendment 704); see also Section E.5. of Chapter III (Trademark) of this Manual.

On November 1, 2009, § 2B5.3 was amended again, this time responding to the Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008, which added statutory sentencing enhancements to 18 U.S.C. § 2320 providing that if an offender causes or attempts to cause serious bodily injury, the statutory maximum term of imprisonment is increased from 10 years to 20 years; if the offender causes or attempts to cause death, the statutory maximum is increased to any term of years (or to life). *See* PRO-IP Act, Pub. L. No. 110-403, § 205, 122 Stat. 4256, 4261-62 (2008). The November 2009 amendment: (i) clarified that the enhancement in § 2B5.3(b)(5), which applies when the offense involved the risk of serious bodily injury, also applies when the offense involved the risk of death; and (ii) increased the minimum offense level in such a situation from level 13 to level 14. *See* U.S.S.G. App. C (Amendment 735). This brought § 2B5.3 back into parallel with § 2B1.1, reflecting the Commission's prior judgment that "aggravating conduct in connection with infringement cases should be treated under the guidelines in the same way it is treated in connection with fraud cases." *Id.* (Amendment 590).

As is discussed in Section C.2. of this Chapter, U.S.S.G. § 2B1.1 is the applicable Guideline for the Economic Espionage Act.

b. Base Offense Level

The base offense level under U.S.S.G. § 2B5.3 is 8.

c. Adjust the Offense Level According to the "Infringement Amount"—U.S.S.G. § 2B5.3(b)(1)

Under U.S.S.G. § 2B5.3(b)(1), the base offense level is adjusted according to the "infringement amount," an estimate of the magnitude of infringement. "Similar to the sentences for theft and fraud offenses, the sentences for defendants convicted of intellectual property offenses should reflect the nature and magnitude of the pecuniary harm caused by their crimes. Accordingly, similar to the loss enhancement in the theft and fraud guideline, the infringement amount in subsection (b)(1) serves as a principal factor in determining the offense level for intellectual property offenses." U.S.S.G. § 2B5.3 cmt. backg'd. The mechanics of calculating the infringement amount are covered in U.S.S.G. § 2B5.3 cmt. n.2.

i. Formula

The infringement amount is generally calculated by multiplying the number of infringing goods by the goods' retail value. *See* U.S.S.G. § 2B5.3 cmt. n.2(A),(B).

If the defendant infringed different types of items, the infringement amount is the sum of the individual infringement amounts for each type of item. *Id.* cmt. n.2(D). The infringement amount for each type of item is calculated independently of the others, including whether the retail value should be that of an infringing (counterfeit) item or an infringed (legitimate) item. *Id.* See Section C.1.c.iii. of this Chapter. The individual infringement amounts are then aggregated into a total infringement amount, which is plugged into the loss table in U.S.S.G. § 2B1.1. See Section C.1.c.v. of this Chapter.

ii. Number of Infringing Items

The number of infringing items may be easy to calculate. Victims or their representatives can often help verify the number when the number depends on whether an item's copyright or trademark has been registered. For a list of industry associations that represent victims, consult Appendix G of this Manual or call CCIPS at (202) 514-1026. When the number of infringing items is difficult or impossible to calculate, however, reasonable estimates are allowed. See U.S.S.G. § 2B5.3, cmt. n.2(E). See also Section C.1.c.iv. of this Chapter.

In cases under 18 U.S.C. § 2318 or § 2320, which involve counterfeit labels that have not been affixed to, or packaging that does not actually enclose or accompany, a good or service, count as the infringing items those labels and packaging which, "had [they] been so used, would appear to a reasonably informed purchaser to be affixed to, enclosing or accompanying an identifiable, genuine good or service." U.S.S.G. § 2B5.3, cmt. n.2(A)(vii). In DMCA cases, count as the infringing items those "circumvention devices" which were used or designed to "access ... [a] copyrighted work." *Id.* cmt. n.2(A)(viii). "'Circumvention devices' are devices used to perform the activity described in 17 U.S.C. 1201(a)(3)(A) and 1201(b)(2)(A)." *Id.* cmt. n.1.

A recurring question is whether the infringement amount should include all the infringing items that the defendant acquired or only those that he provided to another, such as a customer or co-conspirator. For the offenses of trafficking in counterfeit goods and labels, the infringement amount should include all

items the defendant acquired because the term "traffic" is defined to include obtaining control over an infringing item with the "intent to ... transport, transfer, or otherwise dispose of" it. 18 U.S.C. §§ 2320(f)(5), 2318(b)(2). This applies equally if the defendant is convicted of attempting or conspiring to traffic in counterfeit goods. *See* 18 U.S.C. § 2320(a).

Similarly, criminal copyright infringement includes the unauthorized "reproduction or distribution" of copyrighted works (emphasis added), and thus the infringement amount includes all infringing items, regardless of whether they were transferred to others. 17 U.S.C. § 506(a)(1)(B). The bootlegging and camcording statutes also criminalize the production of infringing items, regardless of distribution. *See* 18 U.S.C. §§ 2319A(a)(1), 2319B(a). Finally, the DMCA prohibits the production of infringing items—by circumventing protective technological measures—and does not require distribution. *See* 17 U.S.C. § 1201(a)(1)(A).

Still open is the question of whether and to what extent to include items that are incomplete, such as items in the process of production. This issue is discussed at length in Section E.5. of Chapter III of this Manual (sentencing issues concerning counterfeit marks).

iii. Retail Value

The major issues with determining the retail value are what to do when the items have not been fully manufactured, how to value items that facilitate infringement, which market should be used for reference, and whether to use the value of a counterfeit or a legitimate item. These questions are addressed below.

Incompletely Manufactured Items

How to value items whose manufacture is incomplete is treated in Section E.5. of Chapter III and E.5. of Chapter VI of this Manual.

Items that Facilitate Infringement Such as Labels and DMCA Circumvention Devices

For cases under 18 U.S.C. § 2318 or § 2320 involving counterfeit labels or packaging, the infringement amount is based on the retail value of the infringed item, which is the "identifiable, genuine good or service" to which the label would have been affixed or the packaging would have enclosed or accompanied. U.S.S.G. § 2B5.3 cmt. n.2(A)(vii). For DMCA cases, the

infringement amount is also based on the retail value of the infringed item, which is the "price the user would have paid to access lawfully the copyrighted work, and the 'infringed item' is the accessed work." *Id.* cmt. n.2(A)(viii).

Choosing the Correct Market

"[T]he 'retail value' of an infringed item or an infringing item is the retail price of that item in the market in which it is sold." U.S.S.G. § 2B5.3 cmt. n.2(C). To define the relevant market in which the items are sold, the government should focus on the market's geographic location, whether it exists on the Internet or in real-world storefronts, and whether it is sold in a legitimate market or a black market.

Infringing/Counterfeit vs. Infringed/Authentic Retail Values

Infringing items often trade for much less than authentic items. Using the retail value of one rather than the other can easily mean the difference between months and years in prison, if not between prison and probation. Consequently, whether to use the retail value of counterfeit or authentic items is often the predominant issue at sentencing.

The general rule of fitting the punishment to the harm applies to selecting the retail value. Intellectual property crimes create four basic types of harm: (1) the fraud on consumers who were tricked into buying something inauthentic (at the defendant's prices); (2) the legitimate income that rights holders lost (at legitimate prices) when consumers mistakenly bought the defendant's items; (3) the rights holders' inability to control the use of their property, whether consumers were defrauded or not; and (4) the defendant's unjust enrichment (at the defendant's prices) by using the rights-holder's intellectual property unlawfully.

To value these harms, the law simplified the inquiry into whether the defendant caused or was likely to have caused the victim to lose sales. If so, the maximum measure of harm is the victim's lost sales, which are valued at the victim's own prices. If not, the maximum measure of harm is the defendant's gain, which is valued at what the defendant took in, at his own prices. And if the counterfeit price is hard to determine, then the harm should be computed at the legitimate item's price for ease of calculation.

Originally, the Guidelines directed courts to account for these harms by using only the retail value of infringing (counterfeit) items. *See* U.S.S.G. § 2B5.3(b)(1) & cmt. n.1 & backg'd (1998). But this approach was difficult to apply when

infringing content, such as pirated software or music, had been distributed for free over the Internet, thereby resulting in an infringement amount of $0. Nor did the Guidelines explain how to calculate the retail value of the infringing items when that value was difficult to determine. Notwithstanding the original Guidelines' silence as to a legitimate item's retail value, courts recognized its relevance in a variety of circumstances. The Second Circuit clarified that high-quality fakes should be valued at the retail price and lower-quality fakes should be valued at the counterfeit price. *See United States v. Larracuente*, 952 F.2d 672, 674-75 (2d Cir. 1992). Other courts recognized that a genuine item's price could help determine a counterfeit item's retail value when it otherwise was difficult to determine. *See, e.g., United States v. Bao*, 189 F.3d 860, 866-67 (9th Cir. 1999).

On May 1, 2000, the Guidelines caught up to the case law by concentrating on the harm the defendant caused, whether he displaced the victim's legitimate sales, and how hard it is to calculate the counterfeit's value. *See* U.S.S.G. App. C (Amendments 590, 593). Application Note 2(A) to U.S.S.G. § 2B5.3 now instructs the court to use the retail value of an authentic item if any one of the following situations applies:

> *The infringing item "is, or appears to a reasonably informed purchaser to be, identical or substantially equivalent to the infringed item," U.S.S.G. § 2B5.3 cmt. (n.2(A)(i)(I))*

Differences in appearance and quality therefore matter if they could be ascertained by "a reasonably informed purchaser." *Id*. An infringing item that could fool only an uninformed purchaser would be valued at the counterfeit retail value. *See United States v. Park*, 373 Fed. Appx. 463, 464 (5th Cir 2010) (district court did not clearly err in using retail value of infringed items to calculate Guidelines range after receiving expert testimony that infringing items "would have appeared to a reasonably informed purchaser to be identical or substantially equivalent to the infringed items"); *United States v. Alim*, 256 Fed. Appx. 236, 240-41 (11th Cir. 2007) (same); *United States v. Lozano*, 490 F.3d 1317, 1322-23 (11th Cir. 2007) (same); *United States v. Yi*, 460 F.3d 623, 636-638 (5th Cir. 2006) (district court erred in using retail value of infringed items in part because the infringed and infringing items did not appear "virtually indistinguishable to a reasonably informed purchaser").

The infringing item is a digital or electronic reproduction, U.S.S.G. § 2B5.3 cmt. n.2(A)(i)(II)

For digital or electronic reproductions, use the retail value of the authentic item regardless of whether the reproductions appear authentic to a reasonably informed purchaser. A counterfeit movie DVD with an obviously counterfeit label is valued at the authentic item's retail value, even though nobody would be confused into mistaking the counterfeit for an authentic DVD. Because a digital or electronic reproduction is a perfect substitute for the real thing, whether its outer trappings look legitimate or not, the Commission reasoned that in such cases, "the sale of an infringing item results in a displaced sale of the legitimate, infringed item," making it appropriate to use the value of the infringed items for Guidelines calculations. U.S.S.G. App. C (Amendment 593). Moreover, the guideline simply does not distinguish between types of digital reproduction, such as when the digital or electronic reproduction is not a perfect substitute because its quality was degraded, as with a camcorded movie or a musical song that has been reproduced at a lower sampling rate than CD quality.

The counterfeit was sold at 75% or more of the authentic item's retail price, U.S.S.G. § 2B5.3 cmt. n.2(A)(ii)

The Commission reasoned that counterfeits sold at steep discounts should not be valued the infringed items' price because "the greatly discounted price at which [the counterfeits are] sold suggests that many purchasers of infringing items would not, or could not, have purchased the infringed item in the absence of the availability of the infringing item." U.S.S.G. App. C (Amendment 593). Therefore, counterfeits sold at "not less than 75% of the retail price of the infringed item" may be valued at the infringed items' price. *Id.*; *see also Yi*, 460 F.3d at 637-38 (district court erred in using value of infringed items in part because the infringing items sold for well below 75% of the infringed items' retail price).

The counterfeit's retail value "is difficult or impossible to determine without unduly complicating or prolonging the sentencing proceeding," U.S.S.G. § 2B5.3 cmt. n.2(A)(iii)

Another enumerated situation permitting use of the infringed items' retail value is when the counterfeit's retail is "difficult or impossible to determine without unduly complicating or prolonging the sentencing proceeding." U.S.S.G. § 2B5.3 cmt. n.2(A)(iii); *see also Yi*, 460 F.3d at 638 (district court

erred in using value of infringed items in part because "the retail values of many of the infringing items were not only known to the government but presented at trial"). Moreover, as is discussed in Section C.1.c.iv. of this Chapter, reasonable estimates of the counterfeit retail prices are acceptable, but speculative guesses or overly time-consuming calculations are not.

> *The offense involved illegal interception of satellite cable signals in violation of 18 U.S.C. § 2511, where "the 'retail value of the infringed item' is the price the user of the transmission would have paid to lawfully receive that transmission, and the 'infringed item' is the satellite transmission rather than the intercepting device," U.S.S.G. § 2B5.3 cmt. n.2(A)(iv)*

See United States v. Brereton, 196 Fed. Appx. 688, 691-93 (10th Cir. 2006) (district court did not clearly err in relying on expert testimony that purchasers of pirated DIRECTV access cards had "viewing habits like those in the top ten percent of all DIRECTV customers" and then using the cost for that level of access as the "retail value of the infringed item"). The Commission did not specify why it cited only 18 U.S.C. § 2511 and not other statutes criminalizing the illegal interception of satellite cable signals, such as 47 U.S.C. §§ 553(b)(2) and 605, but neither did it exclude them from the rule's application. *See* U.S.S.G. App. C (Amendment 593).

> *The retail value of the authentic good is a better approximation of the harm than the value of the counterfeit, U.S.S.G. § 2B5.3 cmt. n.2(A)(v)*

See Lozano, 490 F.3d at 1322-23 (district court did not clearly err in using retail value of infringed item after finding this provided a more accurate assessment of the pecuniary harm to the rights holder than the value of the infringing items); *Yi*, 460 F.3d at 637 (error to use infringed items' retail value because it was "not at all clear on which record evidence, if any, the district court based its assessment that the infringed item value provides a more accurate assessment of the pecuniary harm to the trademark owners").

> *The offense involves the display, performance, publication, reproduction, or distribution of a work being prepared for commercial distribution. In a case involving such an offense, the 'retail value*

> *of the infringed [authentic] item' is the value of that item upon its initial commercial distribution, U.S.S.G. § 2B5.3 cmt. n.2(A)(vi)*

This is part of the Sentencing Commission's solution to the so-called "pre-release problem"—that is, how to value an infringing copyrighted work whose infringement occurred before the rights-holder put the authentic work on the market itself. Confronted with widely diverging estimates of the harm caused by pre-release piracy, the Commission determined that a pre-release work's retail value should equal its anticipated legitimate retail value, but that a 2-point upward adjustment should be added for all pre-release offenses. See U.S.S.G. § 2B5.3(b)(2). See also Section C.1.d. of this Chapter.

> *A case under 18 U.S.C. § 2318 or § 2320 that involves a counterfeit label, patch, sticker, wrapper, badge, emblem, medallion, charm, box, container, can, case, hangtag, documentation, or packaging of any type or nature (I) that has not been affixed to, or does not enclose or accompany a good or service; and (II) which, had it been so used, would appear to a reasonably informed purchaser to be affixed to, enclosing or accompanying an identifiable, genuine good or service. In such a case, the "infringed item" is the identifiable, genuine good or service, U.S.S.G. § 2B5.3 cmt. n.2(A)(vii)*

The Sentencing Commission was responding to the directive in the Stop Counterfeiting in Manufactured Goods Act that it address situations in which "the item in which the defendant trafficked was infringing and also was intended to facilitate infringement in another good or service, such as a counterfeit label, documentation, or packaging ...." *See* U.S.S.G. Appendix C (Amendment 682); *cf. United States v. Sung*, 87 F.3d 194, 196 (7th Cir. 1996) (prior to Amendment 682, holding that defendant could only be held liable for the counterfeit shampoo bottles he actually filled, unless the district court found with "reasonable certainty" that he had intended to fill the rest).

> *A case under 17 U.S.C. §§ 1201 and 1204 in which the defendant used a circumvention device. In such an offense, the 'retail value of the infringed item' is the price the user would have paid to access lawfully the copyrighted work, and the 'infringed item' is the accessed work, U.S.S.G. § 2B5.3 cmt. n.2(A)(viii)*

This was the Sentencing Commission's response to the directive in the Stop Counterfeiting in Manufactured Goods Act that it address situations in which "the item in which the defendant trafficked was not an infringing item but

rather was intended to facilitate infringement, such as an anti-circumvention device (sic) ...." *See* U.S.S.G. App. C (Amendment 704). This applies only if the "defendant used a circumvention device and thus obtained unauthorized access to a copyrighted work." *Id*. If the defendant "violated 17 U.S.C. §§ 1201 and 1204 by conduct that did not include use of a circumvention device ... the infringement amount would be determined by reference to the value of the infringing item, which in these cases would be the circumvention device." *Id*.

If any one of the above situations applies, the retail value is that of the infringed (legitimate) item.

If none of these situations apply, the retail value is that of the infringing (counterfeit) item. *See* U.S.S.G. § 2B5.3 cmt. n.2(B) & backg'd; *id*. App. C (Amendment 593). This includes cases involving the unlawful recording of a musical performance in violation of 18 U.S.C. § 2319A. U.S.S.G. § 2B5.3 cmt. n.2(B).

iv. Determining Amounts and Values—Reasonable Estimates Allowed

Any relevant source of information is appropriate in determining the infringing or infringed item's retail value. Actual prices are preferable, such as prices determined from the defendant's price list, prices charged during undercover buys, or actual retail prices for specific items in the legitimate manufacturer's catalogue. Approximations may be necessary, however, and they may include estimations of the average counterfeit prices in the market or region as determined by experts, or the average retail price for a product line in the manufacturer's catalogue.

The same rule applies when determining the number of infringing items: actual counts are preferable, but approximations are appropriate. U.S.S.G. § 2B5.3 explicitly states that reasonable estimates are acceptable. On October 24, 2005, on a temporary, emergency basis, and on November 1, 2006, permanently, Application Note 2(E) was added to U.S.S.G. § 2B5.3:

> (E) Indeterminate Number of Infringing Items.—In a case in which the court cannot determine the number of infringing items, the court need only make a reasonable estimate of the infringement amount using any relevant information, including financial records.

See U.S.S.G. App. C (Amendment 675, 687). The reference to financial records is likely an incorporation of the Tenth Circuit's holding in *Foote*. *See United States v. Foote*, 413 F.3d 1240, 1251 (10th Cir. 2005) (allowing analysis of defendant's bank records to aid in determining infringement amount); *see also United States v. Sweeney*, 611 F.3d 459, 474 (8th Cir. 2010) (holding that district did not clearly err under § 2B5.3 in making a "reasonable estimate" of the infringement amount by starting with the gross revenues of the defendants' company, which sold cable television descramblers); *United States v. Beydoun*, 469 F.3d 102, 105-06 (5th Cir. 2006) (noting under § 2B5.3 only a reasonable estimate of copyright infringement was required).

Although statistical precision is preferable, it is not necessary. For example, in *Sweeney*, the defendants argued that the government had not proved that any of the 178,260 descramblers it sold over a three-year period were "actually used to intercept cable signals illegally," and the "correct infringement amount was therefore $0." *Sweeney*, 611 F.3d at 474. Rejecting this as "sophistry," the Court found that, under the methodology set out in U.S.S.G. § 2B5.3, cmt. n.2(E), "[i]t [was] perfectly reasonable to infer that the majority of these descramblers were in fact used to steal cable programming," even though "the exact number and value of stolen cable transmissions [were] unknown ...." *Id*.

Although U.S.S.G. § 2B5.3 speaks only of estimating the number of infringing items, there is no reason to believe that it abrogates earlier law allowing the estimation of retail values. *E.g., United States v. Brereton*, 196 Fed. Appx. 688, 692-93 (10th Cir. 2006) (citing *Foote*, finding that district court did not clearly err in making reasonable estimate of retail value of pirated DIRECTV access cards); *Foote*, 413 F.3d at 1251 ("[d]istrict courts have considerable leeway in assessing the retail value of the infringing items, and need only make a reasonable estimate of the loss, given the available information") (internal quotation marks and citation omitted); *United States v. Slater*, 348 F.3d 666, 670 (7th Cir. 2003) (confirming that district courts have "considerable leeway in assessing the retail value of the infringing items" and that courts "need only make a reasonable estimate of the loss, given the available information," citing the former U.S.S.G. § 2F1.1, now replaced by § 2B1.1).

v. Cross-Reference to Loss Table in U.S.S.G. § 2B1.1

Once calculated, the infringement amount sets the scope of the enhancement in U.S.S.G. § 2B5.3(b)(1):

- An infringement amount below or up to $2,000 results in no increase;
- An infringement amount above $2,000 and up to $5,000 results in a 1-level increase; and
- An infringement amount above $5,000 increases the offense level according to the loss table in U.S.S.G. § 2B1.1(b)(1) (Theft, Embezzlement, Receipt of Stolen Property, Property Destruction, and Offenses Involving Fraud or Deceit).

When consulting U.S.S.G. § 2B1.1, look only to the loss table in subsection (b)(1); other portions of that guideline—including the base offense level, other offense enhancements, and the commentary—are inapplicable. *See* U.S.S.G. § 1B1.5(b)(2). Moreover, U.S.S.G. § 2B5.3(b)(1)'s citation to the loss table in U.S.S.G. § 2B1.1 does not mean that the infringement amount should equal the victim's loss. Rather, the infringement amount approximates the victim's loss, but need not equal it. *See United States v. Bao*, 189 F.3d 860, 867 (9th Cir. 1999) (finding that district court properly calculated the amount for the loss table in U.S.S.G. § 2F1.1 – which has since been replaced by U.S.S.G. § 2B1.1 – by using the retail value of the counterfeit items and not the loss derived from their production); *United States v. Cho*, 136 F.3d 982 (5th Cir. 1998) (same); U.S.S.G. Appendix C (Amendments 590, 593) (discussing infringement amount as similar to loss and an approximation of harm); *cf. United States v. Koczuk*, 252 F.3d 91, 97 (2d Cir. 2001) (in wildlife case, citing *Cho*, finding that calculation using loss table in U.S.S.G. § 2F1.1 should be based on retail price of endangered species involved, not economic loss caused by offense). On this technical point, *United States v. Sung*, 51 F.3d 92, 95 (7th Cir. 1995) is incorrect when it confuses the infringement amount with the loss incurred. Although the infringement amount is often characterized as describing the "loss" to the victim, it is not necessary for the government to show that the copyright owner suffered any actual pecuniary loss. *See Beydoun*, 469 F.3d at 105 (defendant, who produced booklets of counterfeit cigarette rolling papers with the intent to sell them, was accountable even if he "never sold a single infringing booklet"); *United States v. Powell*, 139 Fed. Appx. 545 (4th Cir. 2005) (applying 2003 Guidelines, finding enhancement under § 2B1.1 table based on infringement amount of more than $250,000 was proper even though the victim suffered no pecuniary loss; sentence vacated and remanded on other grounds).

d. Pre-release Piracy Increases the Offense Level by 2—U.S.S.G. § 2B5.3(b)(2)

Distribution of a copyrighted item before it is legally available to the consumer is more serious than the distribution of already available items. U.S.S.G. App. C (Amendment 675, 687). Consequently, effective October 24, 2005, on a temporary, emergency basis, and permanently on November 1, 2006, the Sentencing Commission added a 2-level enhancement for offenses that involve the display, performance, publication, reproduction, or distribution of a work being prepared for commercial distribution. *See* U.S.S.G. § 2B5.3(b)(2). A "[w]ork being prepared for commercial distribution" has the meaning given in 17 U.S.C.§ 506(a)(3). U.S.S.G. § 2B5.3 cmt. n.1. See also Chapter II of this Manual.

The 2-level increase for pre-release piracy applies not only to the online pre-release offense set forth in 17 U.S.C. § 506(a)(1)(C) (which by definition involves pre-release piracy over publicly-accessible computer networks), but also to any copyright crimes under § 506(a)(1)(A) or (B) that involve pre-release piracy done through any other medium, such as a § 506(a)(1)(A) conviction for selling pirated pre-release movie DVDs.

e. Manufacturing, Importing, or Uploading Infringing Items Increases the Offense Level by 2—U.S.S.G. § 2B5.3(b)(3) [before October 24, 2005: § 2B5.3(b)(2)]

The offense level is increased by 2 levels if the offense involves the "manufacture, importation, or uploading of infringing items." U.S.S.G. § 2B5.3(b)(3). If, after applying § 2B5.3(a), (b)(1), (b)(2), and the 2-level increase in (b)(3), the offense level is less than 12, then it must be increased to 12. U.S.S.G. § 2B5.3(b)(3).

This upward adjustment reflects the need to punish those who introduce infringing goods into the stream of commerce. U.S.S.G. App. C (Amendments 590, 593).

Uploading is particularly troublesome because it not only introduces infringing items into the stream of commerce, but also enables further infringement of the works. U.S.S.G. App. C (Amendments 590, 593). "'Uploading' means making an infringing item available on the Internet or a similar electronic bulletin board with the intent to enable other persons to (A) download or otherwise copy the infringing item; or (B) have access to

the infringing item, including by storing the infringing item as an openly shared file. 'Uploading' does not include merely downloading or installing an infringing item on a hard drive on a defendant's personal computer unless the infringing item is an openly shared file." U.S.S.G. § 2B5.3 cmt. n.1 (Nov. 1, 2006). (Before the October 24, 2005 temporary, emergency amendments, made permanent on November 1, 2006 with minor changes, "uploading" was defined in § 2B5.3's first and third application notes. The 2005 and 2006 amendments consolidated the definition into the first application note and clarified the circumstances in which loading a file onto a computer hard drive constitutes uploading. *See* U.S.S.G. App. C (Amendments 675, 687).)

Manufacturing and importing infringing items are also singled out for a 2-level increase because those actions introduce infringing items into the stream of commerce. U.S.S.G. § 2B5.3 and App. C (Amendments 590, 593).

Although the Guidelines do not define "manufacturing," the important distinction is between manufacturing (which gets the 2-level increase) and mere distribution and trafficking (which do not get an increase unless the conduct also involved importation or uploading). *See United States v. Gray*, 446 Fed. Appx. 569, 570 (4th Cir. 2011) (per curiam) (district court did not clearly err in applying manufacturing enhancement to defendant who "not only bought and resold infringing materials, but ... personally created infringing materials using equipment found in his home"); *Brereton*, 196 Fed. Appx. at 693 (finding that defendant's reprogramming of pirated DIRECTV access cards before selling them justified manufacturing enhancement).

Manufacturing should encompass not only the production of counterfeit trademarked hard goods, but also the performance of counterfeit service-marked services and the production and reproduction of pirated copyrighted works under 17 U.S.C. § 506; counterfeit labels under 18 U.S.C. § 2318; bootleg music recordings under 17 U.S.C. § 2319A; camcorded movies under 18 U.S.C. § 2319B; and illegal circumvention devices under 17 U.S.C. § 1204.

If a defendant conspired with or aided and abetted another person who manufactured, uploaded, or imported infringing items, the defendant can qualify for this 2-level increase even if he did none of these things himself. The increase is triggered by whether the offense involved manufacturing, importation, or uploading, not whether the defendant performed these tasks. *See* U.S.S.G. § 2B5.3(b)(3) ("If the offense involved the manufacture,

importation, or uploading ...") (emphasis added); U.S.S.G. § Ch. 2 (Introductory Commentary) ("Chapter Two pertains to offense conduct.").

f. Offense Not Committed for Commercial Advantage or Private Financial Gain Reduces the Offense Level by 2—U.S.S.G. § 2B5.3(b)(4)

The fourth offense characteristic, located in guideline § 2B5.3(b)(4), decreases the offense level by 2 levels if the offense was not committed for commercial advantage or private financial gain, but the resulting offense level cannot be less than 8.

The defendant bears the burden of proving that he is entitled to this offense characteristic, because it is structured as a decrease rather than an increase. *See generally United States v. Perez*, 418 Fed. Appx. 829, 836 (11th Cir. 2011) *United States v. Ameline*, 409 F.3d 1073, 1086 (9th Cir. 2005) (en banc); *United States v. Dinges*, 917 F.2d 1133, 1135 (8th Cir. 1990); *United States v. Kirk*, 894 F.2d 1162, 1164 (10th Cir. 1990); *United States v. Urrego-Linares*, 879 F.2d 1234, 1238-39 (4th Cir. 1989); *United States v. Herbst*, No. 10-CR-1008-LRR, 2011 WL 794507, at *12 (D. Iowa March 1, 2011).

For a detailed discussion of what qualifies as conduct done for the purposes of commercial advantage or private financial gain, see Section B.4. of Chapter II (Copyright) of this Manual. The interpretation of commercial advantage and private financial gain in copyright cases applies equally to U.S.S.G. § 2B5.3 for any type of intellectual property crime because the statutory and Guidelines definitions are nearly identical. *Compare* U.S.S.G. § 2B5.3 cmt. n.1 (defining terms) *with* 17 U.S.C. § 101 (same).

g. Offense Involving a Counterfeit Drug Increases the Offense Level by 2—U.S.S.G. § 2B5.3(b)(5) (effective November 1, 2013)

In an amendment scheduled to take effect November 1, 2013, if the offense involved a counterfeit drug, the offense level is increased by 2. *See* U.S.S.G. § 2B5.3(b)(5). This will replace the existing § 2B5.3(b)(5), which will be renumbered § 2B5.3(b)(6).

In March 2011, the Office of the Intellectual Property Enforcement Coordinator transmitted a range of legislative proposals to Congress including a number or recommendations to enhance certain Guidelines, including those for counterfeit drugs. *See* Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations (March 2011) ("White Paper"),

available at http://www.whitehouse.gov/sites/default/files/ip_white_paper.pdf. In response, the Food and Drug Administration Safety and Innovation Act, Pub. L. No. 112-144, § 717(b), 126 Stat. 993, 1076 (July 9, 2012), directed the United States Sentencing Commission to review existing penalties for violations of 18 U.S.C. § 2320, and included a general recommendation that the applicable Sentencing Guidelines be increased, particularly for counterfeit drug offenses.

On April 10, 2013, the Commission voted to amend § 2B5.3 to provide the new two-level enhancement when the offense involves a counterfeit drug. This amendment will go into effect on November 1, 2013, unless Congress and the President act to disapprove it. Because the guidelines are advisory only, though, this amendment can be cited before then to courts as a reason for varying from the current guidelines. *See, e.g.*, *United States v. Mateos*, 623 F.3d 1350 (11th Cir. 2010) (Justice O'Connor, sitting by designation, holding that forthcoming changes to the sentencing guidelines inform both the sentencing and reviewing courts on the appropriate sentencing in a given case).

h. Offense Involving Risk of Death or Serious Bodily Injury or Possession of a Dangerous Weapon Increases the Offense Level by 2—U.S.S.G. § 2B5.3(b)(5)

If the offense involved conscious or reckless risk of death or serious bodily injury or possession of a dangerous weapon, the offense level is increased by 2. U.S.S.G. § 2B5.3(b)(5). If the resulting offense level is less than 14, then it must be increased to level 14. *See, e.g., United States v. Maloney*, 85 Fed. Appx. 252 (2d Cir. 2004) (applying 2-level enhancement for possession of a dangerous weapon in connection with conviction under 18 U.S.C. § 2318(a),(c)(3) and § 2, even though defendant was acquitted at trial of a felon-in-possession of a firearm charge). This subsection was last amended in response to the PRO-IP Act of 2008 to include offenses involving risk of death. U.S.S.G. App. C (Amendment 735); PRO-IP Act of 2008, Pub. L. No. 110-403, § 205, 122 Stat. 4256, 4262 (2008). This brought § 2B5.3 back into parallel with § 2B1.1, reflecting the Commission's prior judgment that "aggravating conduct in connection with infringement cases should be treated under the guidelines in the same way it is treated in connection with fraud cases." U.S.S.G. App. C (Amendment 590).

This enhancement was partially motivated by the health and safety risks from counterfeit consumer products such as counterfeit batteries, airplane parts, and pharmaceuticals. *See* U.S.S.G. App. C (Amendments 590, 593).

On April 10, 2013, the Commission voted to amend § 2B5.3 by adding a new § 2B5.3(b)(5) for offenses involving counterfeit drugs and renumbering the current § 2B5.3(b)(5) as § 2B5.3(b)(6). This amendment will go into effect on November 1, 2013, unless Congress and the President act to disapprove it.

i. Offense Involving Counterfeit Military Goods and Services Under Certain Conditions Increases the Offense Level by 2 and Sets a Minimum Offense Level of 14—U.S.S.G. § 2B5.3(b)(7) (effective November 1, 2013)

In an amendment scheduled to take effect November 1, 2013, if the offense involves counterfeit military goods and services the use, malfunction, or failure of which is likely to cause the disclosure of classified information, impairment of combat operations, or other significant harm to a combat operation, a member of the Armed Forces, or to national security, the offense level is increased by 2, and if the resulting offense level is less than level 14, then it is increased to level 14. *See* U.S.S.G. § 2B5.3(b)(7) (proposed). The proposed amendment also adds Commentary to § 2B5.3 to clarify that "other significant harm to a member of the Armed Forces" means significant harm other than serious bodily injury or death. If a military good or service is likely to cause serious bodily injury or death, one would still apply § 2B5.3(b)(5)(A) (conscious or reckless risk of serious bodily injury or death) [after November 1, 2013, § 2B5.3(b)(6)(A)].

Responding in part to the Administration's White Paper, the National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 818(h), 125 Stat. 1298, 1497 (December 31, 2011), amended 18 U.S.C. § 2320 to add a new subsection (a)(3) that prohibits trafficking in counterfeit military goods and services, the use, malfunction, or failure of which is likely to cause serious bodily injury or death, the disclosure of classified information, impairment of combat operations, or other significant harm to a combat operation, a member of the Armed Forces, or national security.

On April 10, 2013, the Commission voted to amend § 2B5.3 to provide the new two-level enhancement and the new minimum offense level of 14 for offenses involving counterfeit military goods and services with the aggravating circumstances set out above and make the corresponding amendment to the

Commentary. These amendments will go into effect on November 1, 2013, unless Congress and the President act to disapprove them. Because the guidelines are advisory only, though, these amendments can be cited before then to courts as a reason for varying from the current guidelines. *See, e.g.*, *Mateos*, 623 F.3d 1350 (Justice O'Connor, sitting by designation, holding that forthcoming changes to the sentencing guidelines inform both the sentencing and reviewing courts on the appropriate sentencing in a given case).

j. Decryption or Circumvention of Access Controls May Increase the Offense Level—U.S.S.G. § 3B1.3

The 2-level enhancement for use of a special skill under U.S.S.G. § 3B1.3 "may apply" if the defendant decrypted or circumvented access controls. U.S.S.G. § 2B5.3 cmt. n.3. On November 1, 2007, the Commission changed this enhancement from mandatory to discretionary, after determining that "not every case involving de-encryption or circumvention requires the level of skill contemplated by the special skill adjustment." *Id.* (Amendment 704).

Because the note quoted above refers only to the circumvention of access controls, it is unclear whether the special skill enhancement also applies to decrypting or circumventing copy controls. There is no policy-related reason to treat access and copy controls differently at sentencing. In fact, U.S.S.G. § 3B1.3 applies to any defendant who commits an intellectual property crime while using a special skill. See Section C.2.i. of this Chapter for a more detailed description of what constitutes a special skill.

This enhancement may not be assessed for use of a special skill if the adjustment under U.S.S.G. § 3B1.1 (Aggravating Role) is also assessed. *See* U.S.S.G. § 3B1.3.

k. Departure Considerations

The fourth application note for § 2B5.3 states that a departure may be warranted if the offense level determined under § 2B5.3 "substantially understates or overstates the seriousness of the offense," such as: (i) when the offense substantially harmed the victim's reputation in a way that is otherwise unaccounted for, including in calculating the infringement amount; (ii) when the offense was in connection with, or in furtherance of, a national or international organized criminal enterprise; and/or (iii) when the method used to calculate the infringement amount overstates the actual pecuniary harm to the victim. These three examples, however, are not exclusive. U.S.S.G. § 2B5.3

cmt. n.4 (noting that this is a "non-exhaustive list of factors" in considering departures); *id*. App. C (Amendments 590, 593, 704). On November 1, 2007, the Commission modified Application Note 4 to address downward as well as upward departures. *Id*. (Amendment 704); *see United States v. Neuman*, 406 Fed. Appx. 847, 852 (5th Cir. 2010) (finding that district court did not abuse its discretion in basing sentence on infringement amount instead of restitution amount where it was clear from the record that the court had duly considered that disparity, and had rejected a downward departure, under U.S.S.G. § 2B5.3 cmt. n.4(C).

On April 10, 2013, the Commission voted to amend the Commentary to § 2B5.3 to add a new departure consideration for any offense sentenced under § 2B5.3 providing that a departure may be warranted if the offense resulted in death or serious bodily injury. *See* U.S.S.G. 2B5.3 cmt. n.4(D) (proposed). This amendment will go into effect on November 1, 2013, unless Congress and the President act to disapprove it. Because the guidelines are advisory only, though, this amendment can be cited before then to courts as a reason for varying from the current guidelines. *See, e.g.*, *Mateos*, 623 F.3d 1350 (Justice O'Connor, sitting by designation, holding that forthcoming changes to the sentencing guidelines inform both the sentencing and reviewing courts on the appropriate sentencing in a given case).

l. Vulnerable Victims—U.S.S.G. § 3A1.1(b)

Intellectual property crime defendants are likely to qualify for an upward adjustment under U.S.S.G. § 3A1.1(b) if they knew or should have known that they were selling counterfeit products to vulnerable victims. A prime example of this would be selling counterfeit pharmaceuticals that are distributed or redistributed to sick patients. *See United States v. Milstein*, 401 F.3d 53, 74 (2d Cir. 2005) (affirming vulnerable victim adjustment for distributing counterfeit and misbranded drugs "to doctors, pharmacists, and pharmaceutical wholesalers, knowing that those customers would distribute the drugs to women with fertility problems and to Parkinson's disease patients").

m. No Downward Departure for the Victim's Participation in Prosecution

The court may not depart downward on the ground that the victim participated in the prosecution. In *United States v. Yang*, 281 F.3d 534 (6th Cir. 2002), *cert. denied*, 537 U.S. 1170 (2003), *on appeal after new sentencing hearing*, 144 Fed. Appx. 521 (6th Cir. 2005), a prosecution for theft of trade

secrets, mail fraud, wire fraud, and money laundering, the trial court departed downward 14 levels on the ground that the victim participated too much in the prosecution, specifically in calculating the loss it suffered. The Sixth Circuit reversed, concluding that "the victim's participation in the prosecution is wholly irrelevant to either the defendant's guilt or the nature or extent of his sentence," and is therefore not a permissible basis for a downward departure. *Yang*, 281 F.3d at 545-46.

2. Offenses Involving the Economic Espionage Act (EEA)

a. Applicable Guideline is § 2B1.1, Except for Attempts and Conspiracies

Unlike most other intellectual property offenses, which are sentenced under U.S.S.G. § 2B5.3, completed EEA offenses (both § 1831 and § 1832) are sentenced under U.S.S.G. § 2B1.1. *See* U.S.S.G. App. A. The choice of U.S.S.G. § 2B1.1 instead of U.S.S.G. § 2B5.3 likely reflects the idea that EEA offenses are primarily about stolen property rather than infringement. The superficial difference between stealing and infringement is that one physically dispossesses the victim of his property and the latter does not. However, the EEA punishes those who steal trade secrets without dispossessing the victim of his trade secret, and even after a trade secret is physically stolen, the victim may still use the information itself. The overlap between misappropriation and infringement therefore makes U.S.S.G. § 2B1.1 an interesting fit for the EEA.

An EEA attempt or conspiracy is sentenced under U.S.S.G. § 2X1.1 (Conspiracies, Attempts, and Solicitations), which uses the offense level calculated under U.S.S.G. § 2B1.1 and decreases the base offense level 3 levels "unless the defendant completed all the acts the defendant believed necessary for successful completion of the substantive offense or the circumstances demonstrate that the defendant was about to complete all such acts but for apprehension or interruption by some similar event beyond the defendant's control." U.S.S.G. § 2X1.1(b)(1), (2). The 3-point reduction will rarely apply in EEA attempt cases resulting from undercover stings because in those operations the defendant has generally completed all necessary acts short of the actual receipt of what the defendant believed was a trade secret.

b. Base Offense Level—U.S.S.G. § 2B1.1(a)

The base offense level for a completed EEA crime is 6. U.S.S.G. § 2B1.1(a)(2).

c. Loss—U.S.S.G. § 2B1.1(b)(1)

The defendant's sentence is driven largely by the value of the misappropriated property. Under U.S.S.G. § 2B1.1(b)(1), the offense level increases according to the amount of the loss.

i. Use Greater of Actual or Intended Loss

This loss figure is "the greater of actual loss or intended loss." U.S.S.G. § 2B1.1 cmt. n.3(A). "Actual loss" is "the reasonably foreseeable pecuniary harm that resulted from the offense," whereas "intended loss (I) means the pecuniary harm that was intended to result from the offense; and (II) includes intended pecuniary harm that would have been impossible or unlikely to occur (e.g., as in a government sting operation, or an insurance fraud in which the claim exceeded the insured value)." *Id.* cmt. n.3(A)(i-ii).

ii. Reasonable Estimates Acceptable

Whatever method is chosen to calculate loss, the government's calculation need not be absolutely certain or precise. "The court need only make a reasonable estimate of the loss." U.S.S.G. § 2B1.1 cmt. n.3(C).

iii. Methods of Calculating Loss

Guideline § 2B1.1's application notes outline a number of general methods for calculating the loss, many of which are included as methods to estimate the loss:

- "[T]he reasonably foreseeable pecuniary harm that resulted from the offense," U.S.S.G. § 2B1.1 cmt. n.3(A)(i)
- "The fair market value of the property unlawfully taken, copied, or destroyed; or, if the fair market value is impracticable to determine or inadequately measures the harm, the cost to the victim of replacing that property," *Id.* n.3(C)(i)
- "In the case of proprietary information (e.g., trade secrets), the cost of developing that information or the reduction in value of that information that resulted from the offense," *Id.* n.3(C)(ii)
- "The cost of repairs to damaged property," *Id.* n.3(C)(iii)
- "The approximate number of victims multiplied by the average loss to each victim," *Id.* n.3(C)(iv)
- "The reduction that resulted from the offense in the value of equity securities or other corporate assets," *Id.* n.3(C)(v)

- "More general factors, such as the scope and duration of the offense and revenues generated by similar operations," *Id*. n.3(C)(vi)
- "[T]he gain that resulted from the offense as an alternative measure of loss[,] only if there is a loss but it reasonably cannot be determined," *Id*. n.3(B)

On November 1, 2009, the Commission amended Application Note 3(C), adding the word "copied" to subdivision (i), and inserting a new subdivision (ii) dealing specifically with proprietary information. U.S.S.G. App. C (Amendment 726). The first change addressed situations in which the owner of proprietary information actually retains possession, but because the information is unlawfully copied and/or disseminated, the information's value declines. In such a case, the court may use the fair market value of the copied information in calculating loss. The second change was simply an effort to provide some direct explanation of how to estimate loss in a trade secrets case. *Id*.

Nevertheless, in a trade secrets case, calculating the loss can be complicated. First, consider the situations under which the defendant can be convicted: (a) merely conspiring to misappropriate a trade secret that the victim has not fully exploited to create a product; (b) receiving a trade secret, but not using the trade secret; (c) stealing a trade secret at no cost; (d) stealing a trade secret for an agreed-upon bribe; (e) receiving a trade secret and using it to create a product that has not been completed; (f) receiving a trade secret, using it to create a product, introducing the product, but not yet selling it; (g) receiving a trade secret, using it to create a product, and selling the product at a loss; (h) receiving the trade secret, using it, and selling the product at a profit, while the victim continues to profit from its own sales; and (i) receiving the trade secret, using it, and selling a product that displaces the victim's sales. These situations do not exhaust the possibilities. They illustrate, however, several complicating factors:

- whether the defendant paid anything for the secret;
- whether the defendant was paid anything for the secret;
- whether the defendant used the secret;
- whether the defendant used the secret and made money from its use; and
- whether the victim's sales decreased, increased, or increased at a lower rate than they would have had the misappropriation not occurred.

The final complicating factor is that trade secrets are, by definition, not traded in an open market that allows the easy calculation of a trade secret's price or value.

The variety of misappropriation scenarios, the variety of evidence available, and the broad principles of valuing trade secrets in criminal and civil law lead to one clear recommendation: prosecutors, agents, and courts should consider the variety of methods by which a trade secret can be valued, develop whatever evidence is reasonably available, and then be pragmatic about choosing which method to use, as long as it is equitable, appropriately punitive, and supported by the evidence. The cases bear this out.

Criminal Cases

Few reported federal criminal decisions describe how to value trade secrets, but those that do tend to focus on the trade secret's research and development costs.

In *United States v. Four Pillars Enter. Co.*, 253 Fed. Appx. 502, 512 (6th Cir. 2007), the defendant company stole more than sixty adhesive formulas from victim Avery Dennison. At sentencing, an Avery employee testified that the research and development costs for the formula totaled $869,300. The Sixth Circuit found no error in the district court's decision to accept this cost model.

In *United States v. Ameri*, 412 F.3d 893 (8th Cir. 2005), an employee stole his employer's proprietary software, which the evidence showed was at the heart of a $10 million contract, had no verifiable fair market value because it was not available separately, alternatively had a fair market value of $1 million per copy, and was developed for about $700,000. *Id*. at 900. Faced with these figures, the Eighth Circuit affirmed the trial court's loss estimate of $1.4 million, which appears to be the $700,000 in development costs times 2, the number of copies the defendant made. *Id*. at 900-01.

Finally, *United States v. Kwan*, No. 02 CR. 241(DAB), 2003 WL 22973515 (S.D.N.Y. Dec. 17, 2003), considered whether "proprietary" "hotel contact lists, hotel rate sheets, travel consortium contact lists, travel consortium rate sheets, and cruise operator rate sheets"—all useful in the travel industry—met the jurisdictional threshold for interstate transportation of stolen property under 18 U.S.C. § 2314 by being worth more than $5,000. *Id*. at *1. The court found most persuasive an argument for a value over $5,000 based on

the documents' cost of production, which it estimated by noting the salary of people who created the documents and the amount of time they would have spent gathering the information and creating the documents. *Id.* at *9 & n.12. In all these cases, the loss or market value was defined largely by development costs.

Some civil trade secret cases have measured the replacement cost using the victim's research and development costs. *See Salsbury Labs., Inc. v. Merieux Labs., Inc.*, 908 F.2d 706, 714-15 (11th Cir. 1990) (holding that research and development costs for misappropriated vaccine were a proper factor to determine damages); *cf. University Computing Co. v. Lykes-Youngstown Corp.*, 504 F.2d 518, 538 (5th Cir. 1974) (holding that development costs should be taken into consideration with a number of factors, including "the commercial context in which the misappropriation occurred"). *But see Softel, Inc. v. Dragon Med. & Scientific Commc'ns, Inc.*, 118 F.3d 955, 969 (2d Cir. 1997) (holding that it is usually appropriate to measure damages based on development costs and importance of secret to plaintiff only after a defendant completely destroys the value of the trade secret).

An interesting exception to using development costs to value trade secrets is *United States v. Pemberton*, 904 F.2d 515 (9th Cir. 1990), in which a legitimate buyer's price was selected. After the defendant was convicted for receiving stolen property, namely technical landscape and irrigation design drawings for a 450-acre commercial development, the trial court had to select among valuation methods, including valuing the drawings at what the drawings were purportedly worth to defendant—zero; the $1,200 cost of the materials on which they were drawn; the $65,000 cost of replacing the drawings in full; and the $118,400 contract price for the drawings (80 percent of the full contract price, given that the drawings were 80 percent complete when stolen). *Id.* at 516 & n.1, 517. Without a price from an open market, since the drawings were unique, the appellate court affirmed the trial court's choice of the $118,400 contract price. *Id.* at 517.

Why use the buyer's price in *Pemberton* rather than the development costs, as had been done in the *Wilson*, *Ameri*, and *Kwan* cases? There appear to be three differences. First, in *Pemberton* the buyer's price came from a legitimate market transaction rather than a black-market transaction that would have undervalued the property. Second, in *Pemberton*, the buyer's price was apparently higher than the development costs. Third, and this is related to the second point, in *Pemberton* the drawings that were stolen likely could have been used for one

project only, the real estate development by the legitimate buyer, whereas the trade secrets in *Wilson*, *Ameri*, and *Kwan* included general information that could have been used over and over again by illegitimate buyers. Research and development costs for a one-off project are likely to be less than the legitimate buyer's price (since this is the only opportunity the trade-secret holder can recover his overhead), whereas research and development costs for a replicable product or service will likely exceed a legitimate buyer's price (since the trade-secret holder can recover his overhead through repeated sales).

Another possible measure of loss in trade secrets cases is actual pecuniary loss. In *United States v. Wilkinson*, 590 F.3d 259 (4th Cir. 2010), the defendant pled guilty to several charges, including conspiracy to steal trade secrets, for his scheme to obtain fuel contracts from the Defense Energy Support Center (DESC) by paying a competitor's employee for confidential bid information which would enable the defendant's company to underbid the competitor. The Fourth Circuit remanded for resentencing, finding that the district court had failed to consider properly the government's evidence of actual loss, even though the DESC never actually ended up paying out on the tainted contracts. The government's expert witness calculated the loss based on the DESC's administrative costs in preparing new bid packages, making spot purchases of fuel while it waited to award replacement contracts, and the ultimately higher costs DESC faced for the untainted replacement contracts. *Id*. at 265.

Civil Cases

Prosecutors should also be aware of how civil cases measure losses from trade secret misappropriation. *See supra*; *cf. United States v. Olis*, 429 F.3d 540, 546 (5th Cir. 2005) (holding that "[t]he loss guideline [in U.S.S.G. § 2B1.1] is skeletal because it covers dozens of federal property crimes," and therefore "[t]he civil damage measure [for securities fraud] should be the backdrop for criminal responsibility both because it furnishes the standard of compensable injury for securities fraud victims and because it is attuned to stock market complexities").

Unfortunately, beyond reinforcing the criminal cases' use of research and development costs, civil measures of damages provide little hard and fast guidance. The Uniform Trade Secrets Act echoes the Sentencing Guidelines' generalities:

> Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by

misappropriation that is not taken into account in computing actual loss.

Uniform Trade Secrets Act § 3(a) (1985); *see also Mike's Train House, Inc. v. Lionel, L.L.C.*, 472 F.3d 398, 413-15 (6th Cir. 2006) (a plaintiff which is able to prove that it was damaged but that the defendant's unjust enrichment exceeded the proven damages to plaintiff, is able to recover his own damages plus, to the extent not duplicative in amount, the defendant's unjust enrichment). In determining damages under the Uniform Trade Secrets Act, courts base the trade secret's market value on the victim's loss or the defendant's gain, depending on which measure appears to be more reliable or greater given the particular circumstances of the theft. *See Vermont Microsystems, Inc. v. Autodesk Inc.*, 138 F.3d 449, 452 (2d Cir. 1998); *University Computing Co. v. Lykes-Youngstown Corp.*, 504 F.2d 518 (5th Cir. 1974); *Healthcare Advocates v. Affordable Healthcare Options*, No. 09-5839, 2010 WL 4665956, at *2 (E.D. Pa. Nov. 18, 2010); Milgrim on Trade Secrets § 15.02(3)(c) (2012). With such broad principles, "the general law as to the proper measure of damages in a trade secrets case is far from uniform." *Telex Corp. v. International Bus. Machs. Corp.*, 510 F.2d 894, 930 (10th Cir. 1975) (concerning misappropriation of trade secrets and confidential information relating to electronic data processing systems).

As might be expected, civil cases use a variety of methods to value trade secrets:

- the value placed on the trade secrets by the parties;
- the victim's lost profits;
- the defendant's realized profits;
- the defendant's saved costs from misappropriation;
- the research and development costs for the trade secret; and
- a reasonable royalty to the victim, when there was otherwise no gain or loss.

1 Richard Raysman & Peter Brown, *Computer Law: Drafting and Negotiating Forms* § 6.03A (2012). When there is evidence for more than one measure, "the court will frequently award that amount which is most beneficial to the injured party." *Id.*

Civil cases often note that if the victim's loss were the only appropriate measure of damages, someone caught red-handed stealing trade secrets could not be punished if he had not yet used the information to the owner's detriment.

As a result, in such circumstances most Uniform Trade Secrets Act cases have computed the trade secret's market value by focusing on the defendant's gain. *See, e.g., University Computing*, 504 F.2d at 536 (holding that damages for misappropriation of trade secrets are measured by the value of the secret to the defendant "where the [trade] secret has not been destroyed and where the plaintiff is unable to prove specific injury"); *Salisbury Labs., Inc. v. Merieux Labs., Inc.*, 908 F.2d 706, 714 (11th Cir. 1990) (ruling that under Georgia's UTSA, damages for misappropriation of trade secrets should be based on the defendant's gain); *SKF USA Inc. v. Bjerkness*, 636 F. Supp. 2d 696 (N.D. Ill. 2009). Under the more recent Federal Sentencing Guidelines, the court may use a defendant's gain as a loss for the victim in certain circumstances. See U.S.S.G. § 2B1.1 cmt. n.3(B) (2012).

The Uniform Trade Secrets Act also provides that damages may be based, as with patent infringement, on a "reasonable royalty"—that is, the amount the thief would have had to pay the victim in licensing or royalty fees had he legitimately licensed the stolen technology:

> In lieu of damages measured by any other methods, the damages caused by misappropriation may be measured by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret.

Uniform Trade Secrets Act § 3(a) (1985). *See, e.g., University Computing*, 504 F.2d at 537. When the defendant has not yet realized sufficient profit to readily indicate the stolen information's market value, the preferred estimate is the "reasonable royalty" (or "forced licensing") measure. *See Vitro Corp. of Am. v. Hall Chem. Co.*, 292 F.2d 678, 682-83 (6th Cir. 1961); *see also Vermont Microsystems, Inc. v. Autodesk, Inc.*, 138 F.3d 449, 450 (2d Cir. 1998). Other federal cases using the "reasonable royalty" method include *Mid-Michigan Computer Sys., Inc. v. Marc Glassman, Inc.*, 416 F.3d 505, 510-13 (6th Cir. 2005); *Molex, Inc. v. Nolen*, 759 F.2d 474 (5th Cir. 1985); *University Computing Co.*, 504 F.2d 518; *Secure Energy, Inc. v. Coal Synthetics, LLC*, 708 F. Supp. 2d 923, 931-32 (E.D. Mo. 2010); *LinkCo, Inc. v. Fujitsu Ltd.*, 232 F. Supp. 2d 182, 186-87 (S.D.N.Y. 2002); *Carter Prods., Inc. v. Colgate-Palmolive Co.*, 214 F. Supp. 383 (D. Md. 1963).

But calculating a reasonable royalty may prove more difficult and may unduly prolong or complicate sentencing in cases where the defendant has not

yet manifested his intention to use the stolen technology and there is no readily ascertainable benchmark for determining a reasonable royalty.

Practical Guidance on Gathering Evidence

Because of the flexible nature of valuing trade secrets, prosecutors and investigators should try to obtain the following types of evidence, if available and applicable:

- the amount the defendant paid for the trade secret;
- the amount for which the defendant sold or tried to sell the trade secret;
- the amount for which similar trade secret information sold in the legitimate open market (such as the merger/acquisition price for the trade secret);
- a reasonable royalty, based on what a willing buyer would pay a willing seller for the technology in an arms-length transaction;
- the trade secret owner's research and development costs;
- the market price that the defendant actually received or paid in exchange for the technology; and
- any other methodology that calculates the reasonably foreseeable pecuniary losses caused by the defendant's conduct.

d. Intent to Benefit a Foreign Government, Instrumentality, or Agent—U.S.S.G. § 2B1.1(b)(5)

The offense level is increased two points if the defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality, or foreign agent. *See* U.S.S.G. § 2B1.1(b)(5). As discussed below, § 2B1.1(b)(5) will be superseded by a new § 2B1.1(b)(12) on November 1, 2013.

e. Intent to Transport or Transmit the Trade Secret out of the United States or to Benefit a Foreign Government, Instrumentality, or Agent—U.S.S.G. § 2B1.1(b)(12) (effective November 1, 2013)

In amendments scheduled to take effect November 1, 2013, the offense level is increased two points if the defendant knew or intended that the trade secret would be transported or transmitted out of the United States. *See* U.S.S.G. § 2B1.1(b)(12)(A) (proposed). Alternatively, the offense level is increased four points if the defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality, or foreign agent, and if the resulting offense level is less than level 14, it is increased to level 14. *See* U.S.S.G. § 2B1.1(b)(12)(B) (proposed).

In March 2011, the Office of the Intellectual Property Enforcement Coordinator transmitted a range of legislative proposals to Congress including a number or recommendations to enhance certain Guidelines, including those for theft of trade secrets. *See* Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations (March 2011), *available at* http://www.whitehouse.gov/sites/default/files/ip_white_paper.pdf. In response, the Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. No. 112-269, § (3)(a), 126 Stat. 2442, 2442-43 (January 14, 2013), directed the United States Sentencing Commission to "review and, if appropriate, amend" the guidelines "applicable to persons convicted of offenses relating to the transmission or attempted transmission of a stolen trade secret outside of the United States or economic espionage, in order to reflect the intent of Congress that penalties for such offenses under the Federal sentencing guidelines and policy statements appropriately, reflect the seriousness of these offenses, account for the potential and actual harm caused by these offenses, and provide adequate deterrence against such offenses." On April 10, 2013, the Commission voted to amend § 2B1.1 to provide the new two-level enhancement when a trade secret is transmitted outside the United States, and the new four-level enhancement—with a minimum level of 14—when the trade secret theft is intended to benefit a foreign government. These amendments will go into effect on November 1, 2013, unless Congress and the President act to disapprove them. Because the guidelines are advisory only, though, these amendments can be cited before then to courts as reasons for varying from the current guidelines. *See, e.g.*, *United States v. Mateos*, 623 F.3d 1350 (11th Cir. 2010) (Justice O'Connor, sitting by designation, holding that forthcoming changes to the sentencing guidelines inform both the sentencing and reviewing courts on the appropriate sentencing in a given case).

f. Sophisticated Means—U.S.S.G. § 2B1.1(b)(10)(C)

If the offense involved "sophisticated means," the offense level is increased by 2 levels, and if the resulting offense is less than 12, it must be increased to 12. U.S.S.G. § 2B1(b)(10)(C). "'[S]ophisticated means' means especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense," which includes "hiding assets or transactions," among other things. *Id.* cmt. n.8(B).

The sophisticated means enhancement will often apply to trade secret offenses because these crimes are frequently committed by corporate insiders who have the need and opportunity to take extensive precautions to shield

their actions from their employers. A defendant can receive the adjustment for sophisticated means in addition to the adjustment for use of a special skill under U.S.S.G. § 3B1.3. *See United States v. Ojemon*, 465 Fed. Appx. 69, 71-72 (2d Cir. 2012); *United States v. Rice*, 52 F.3d 843, 851 (10th Cir. 1995) ("The purpose of the special skill enhancement is to punish those criminals who use their special talents to commit crime. In contrast, the sophisticated means and more than minimal planning enhancements [in predecessor guideline to § 2B1.1] are designed to target criminals who engage in complicated criminal activity because their actions are considered more blameworthy and deserving of greater punishment than a perpetrator of a simple version of the crime. We therefore see no double counting here."); *United States v. Olis*, 429 F.3d 540, 549 (5th Cir. 2005), on remand, No. H-03-217-01, 2006 WL 2716048 (Sep. 22, 2006) (upholding loss calculation based on special skill and sophisticated means, but reducing resulting prison time under the U.S.S.G § 3553(a) factors); *United States v. Minneman*, 143 F.3d 274, 283 (7th Cir. 1998).

g. Upward Departure Considerations—U.S.S.G. § 2B1.1 cmt. n.19(A)

A non-exhaustive list of factors in which an upward departure should be considered is set forth in Application Note 19 to U.S.S.G. § 2B1.1. The factors that are most likely to be relevant in a trade secret case are intending, risking, and causing non-monetary harm, such as emotional harm, because many EEA cases involve disgruntled employees or former employees out for revenge. U.S.S.G. § 2B1.1 cmt. n.19(i),(ii).

h. Downward Departure Considerations—U.S.S.G. § 2B1.1 cmt. n.19(C)

Application Note 19(C) to U.S.S.G. § 2B1.1 suggests that a downward departure may be warranted if the offense level "substantially overstates the seriousness of the offense." EEA defendants are likely to raise this as a basis for downward departure if the loss amount greatly outweighs the amount of the actual or intended gain or loss, as sometimes happens when the trade secret is valued by research and development costs.

i. Abuse of a Position of Trust—U.S.S.G. § 3B1.3

Trade secret offenses committed by corporate insiders often deserve the 2-level adjustment for abuse of a position of trust under U.S.S.G. § 3B1.3. The adjustment is appropriate when the defendant had "professional or managerial

discretion (i.e., substantial discretionary judgment that is ordinarily given considerable deference)" and the position of trust "contributed in some significant way to facilitating the commission or concealment of the offense." *Id*. cmt. n.1. A defendant can receive the enhancements for abuse of a position of trust and sophisticated means simultaneously. *See United States v. Ratliff*, 376 Fed. Appx. 830, 836-41 (10th Cir. 2010); *cf. United States v. Straus*, 188 F.3d 520, 1999 WL 565502, at *5 (10th Cir. 1999) (holding that abuse-of-trust and more-than-minimal-planning enhancements, the latter in a predecessor to U.S.S.G. § 2B1.1(b)(10)(C), can be applied to same conduct simultaneously).

j. Use of Special Skill—U.S.S.G. § 3B1.3

Trade secret defendants who use their specialized technical knowledge to understand and use the misappropriated trade secret will often qualify for a 2-level adjustment for use of a special skill under U.S.S.G. § 3B1.3. *See, e.g., United States v. Lange*, 312 F.3d 263, 270 (7th Cir. 2002) ("Drafting skills, including the use of AutoCAD, are 'not possessed by members of the general public', require time to master, and played a central role in the offense. A mechanical drafter is in the same category as a pilot or demolition expert—for those skills, too, may be learned outside the academy. The enhancement was proper.").

"'Special skill' refers to a skill not possessed by members of the general public and usually requiring substantial education, training, or licensing. Examples would include pilots, lawyers, doctors, accountants, chemists, and demolition experts." U.S.S.G. § 3B1.3 cmt. n.4. Special skill includes any type of special skill, not just one gained through advanced education. In *Lange*, it applied to a mechanical drafter, an EEA defendant who committed his offense using his associate's degree in graphic design and his ability to work with his former employer's engineering drawings in AutoCAD. *Lange*, 312 F.3d at 270.

A defendant can receive the adjustment for use of a special skill in addition to the adjustment for sophisticated means under U.S.S.G. § 2B1.1(b)(9)(C). *See Ojemon*, 465 Fed. Appx. at 71-72.

k. No Downward Departure for Victim's Participation in Developing the Case

As noted in Section C.1.k. of this Chapter, the court may not depart downward on the ground that the victim participated in the prosecution.

D. Restitution

Victims have a right to "full and timely restitution as provided in law." 18 U.S.C. § 3771(a)(6). "All who investigate and prosecute criminal cases play an important role in determining whether restitution is full and timely. The scope of the victim's losses, the nexus between the victim's losses and the crimes charged, what happened to ill-gotten gains, and the defendant's ability to pay are all integral to the criminal prosecution. Restitution should be considered early in the investigation and throughout the prosecution." U.S. Dep't of Justice, *Attorney General Guidelines for Victim and Witness Assistance*, Art. V, H (2012), *available at* http://www.justice.gov/olp/pdf/ag_guidelines2012.pdf.

In intellectual property cases, there are two types of victim: the owner of the intellectual property that was infringed or misappropriated, and any consumer who was lured into purchasing the infringing goods by fraud. Both types of victim usually qualify for restitution if they have suffered a loss.

This section discusses restitution for intellectual property crimes. For more detailed guidance on restitution principles and procedures, prosecutors should consult the *Attorney General Guidelines for Victim and Witness Assistance*, cited above, as well as the U.S. Department of Justice, *Prosecutor's Guide to Criminal Monetary Penalties: Determination, Imposition and Enforcement of Restitution, Fines & Other Monetary Impositions* (2003) (hereinafter, *Prosecutor's Guide to Criminal Monetary Penalties*), *available at* http://dojnet.doj.gov/usao/eousa/ole/usabook/mone/.

1. Restitution is Available—and Often Required—in Intellectual Property Prosecutions

Most criminal intellectual property defendants must pay their victims restitution.

Intellectual property offenses in Title 18 require restitution under the Mandatory Victims Restitution Act of 1996 ("MVRA"), codified in part at 18 U.S.C. § 3663A ("Mandatory restitution to victims of certain crimes"). Under the MVRA, restitution is mandatory following any "offense against property under [Title 18] ... including any offense committed by fraud or deceit ... in which an identifiable victim or victims suffered a pecuniary loss." 18 U.S.C. § 3663A(c)(1)(A)(ii),(B). For offenses committed on or after October 13, 2008, the PRO-IP Act of 2008 made this explicit, creating a new section, 18

U.S.C. § 2323, dealing specifically with forfeiture, destruction and restitution for intellectual property offenses, which provides:

> (c) **Restitution.** — When a person is convicted of an offense under section 506 of title 17 or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of this title, the court, pursuant to sections 3556, 3663A, and 3664 of this title, shall order the person to pay restitution to any victim of the offense as an offense against property referred to in section 3663A(c)(1)(A)(ii) of this title.

18 U.S.C. § 2323(c); PRO-IP Act of 2008, Pub. L. No. 110-403, § 206, 122 Stat. 4256, 4263 (2008). The restitution provisions in the PRO-IP Act superseded an amendment passed only two years earlier in the Stop Counterfeiting in Manufactured Goods Act which made restitution mandatory for violations of 18 U.S.C. § 2320. *See* Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1, 120 Stat. 285, 286 (2006); 18 U.S.C. § 2320(b)(4) (effective March 16, 2006 through October 12, 2008).

The enactment of 18 U.S.C. § 2323 codified a longstanding body of case law. Intellectual property crimes are offenses against property in two senses: some defraud unwitting customers into paying money for infringing products, and all involve intellectual property, which is property as much as any tangible property. *See, e.g., United States v. Carpenter*, 484 U.S. 19, 26 (1987) (stating that confidential information, another type of intangible property, has "long been recognized as property"); *United States v. Trevino*, 956 F.2d 276, 1992 WL 39028 (9th Cir. 1992) (table) (in counterfeit trademark prosecution, affirming order of restitution to nuclear power plant victim that had purchased counterfeit circuit breakers). The handful of cases on point confirmed that intellectual property offenses are "offense[s] against property" for the purpose of § 3663A. *See Beydoun*, 469 F.3d at 107 (noting that a conviction under 18 U.S.C. § 2320 for trafficking in counterfeit cigarette papers was an "offense against property" under 18 U.S.C. § 3663A and thus required mandatory restitution, but finding that the district court calculated incorrectly the amount of restitution); *United States v. Chalupnik*, 514 F.3d 748, 751-52 (8th Cir. 2008) (similarly, noting that a conviction under 17 U.S.C. § 506 and 18 U.S.C. § 2319 for criminal copyright infringement was an "offense against property" under 18 U.S.C. § 3663A, but faulting the district court's calculation of restitution); *United States v. Chay*, 281 F.3d 682, 686 (7th Cir. 2002) (noting that a conviction under 18 U.S.C. § 2318(a) for trafficking in

counterfeit documents and packaging for computer programs was an "offense against property" under 18 U.S.C. § 3663A and thus required mandatory restitution); *United States v. Hanna*, No. 02 CR. 1364-01(RWS), 2003 WL 22705133, at *3 (S.D.N.Y. Nov. 17, 2003) (stating that a conviction under 18 U.S.C. § 2320 for trafficking in counterfeit trademarked handbags and other goods requires full restitution under 18 U.S.C. §§ 3663A, 3664); *see also United States v. Cho*, 136 F.3d 982, 983 (5th Cir. 1998) (mentioning restitution in trademark counterfeiting case); *United States v. Manzer*, 69 F.3d 222, 229-30 (8th Cir. 1995) (upholding restitution award of $2.7 million in mail fraud, wire fraud, and copyright infringement prosecution for the sale of modification and cloning packages for unauthorized decryption of premium channel satellite broadcasts); *United States v. Sung*, 51 F.3d 92, 96 (7th Cir. 1995) (mentioning restitution in trademark counterfeiting case); *United States v. Bohai Trading Co.*, 45 F.3d 577, 579 (1st Cir. 1995) (same—restitution amount of $100,000); *United States v. Hicks*, 46 F.3d 1128, 1995 WL 20791, at *3 (4th Cir. 1995) (table) (upholding restitution award in satellite decryption and copyright case).

These cases support the proposition that restitution is mandatory even for intellectual property offenses committed prior to enactment of § 2323 on October 13, 2008. Restitution also is mandatory for trademark violations committed between passage of the Stop Counterfeiting in Manufactured Goods Act on March 16, 2006, and passage of the PRO-IP Act on October 13, 2008, under the version of 18 U.S.C. § 2320 in effect during that period. *See* Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 108-482, § 1, 120 Stat. 285, 286 (2006); 18 U.S.C. § 2320(b)(4) (effective March 16, 2006 through October 12, 2008).

There are two statutory exceptions to mandatory restitution in § 3663A: "if (A) the number of identifiable victims is so large as to make restitution impracticable; or (B) determining complex issues of fact related to the cause or amount of the victim's losses would complicate or prolong the sentencing process to a degree that the need to provide restitution to any victim is outweighed by the burden on the sentencing process." 18 U.S.C. § 3663A(c)(3). Defendants can be expected to argue for one or both of these exceptions in cases of online copyright piracy that involve a large number of copyrighted works owned by a large number of victims, in cases involving retail counterfeit goods that were sold to a large number of defrauded customers, and in trade secret cases that involve complex issues of valuation. "This 'exception' was

intended to be used sparingly, and the court is expected to use every means available, including a continuance of the restitution determination of up to 90 days, if necessary, to identify as many victims and harms to those victims as possible." *Prosecutor's Guide to Criminal Monetary Penalties* at 28 (citing 18 U.S.C. § 3664(d)(5) and *United States v. Grimes*, 173 F.3d 634 (7th Cir. 1999)). Department policy also requires that when this exception does apply, "where forfeited assets are involved, prosecutors should consult with the Criminal Division's Asset Forfeiture and Money Laundering Section (AFMLS) to determine the most effective way of returning forfeited assets to victims," and "[i]n cases with multiple defendants, the court should be asked to address joint and several liability." U.S. Dep't of Justice, *Attorney General Guidelines for Victim and Witness Assistance*, Art. V, H.1.g (2012). Prosecutors should also ask the court to order restitution "for those victims and harms the court can identify," *Prosecutor's Guide to Criminal Monetary Penalties* at 30 (discussing similar exception for discretionary restitution). How to ensure restitution in such situations is addressed below in the discussion of determining the restitution amount.

Another possible exception to mandatory restitution may exist for criminal trademark, service mark, and certification mark cases under 18 U.S.C. § 2320 in which the mark-holder neglected to use the ® symbol (or other proper notice) and the defendant lacked actual notice that the mark was registered. In those cases, however, even though restitution might not be awarded to the mark-holder, it should still be awarded to any customers of the defendant who were defrauded into buying what they thought were authentic goods or services. See Section E.3. of Chapter III of this Manual.

In addition, certain intellectual property offenses are simply not covered by the mandatory restitution provisions in 18 U.S.C. § 3663A, which apply only to an "offense against property under this title [18]." 18 U.S.C. § 3663A(c)(1)(A)(ii). First, this excludes non-Title 18 offenses, such as violations of the DMCA, *see* 17 U.S.C. § 1204, and unauthorized reception of cable and satellite service, *see* 47 U.S.C. §§ 553(b)(2), 605.

Second, this excludes even Title 18 crimes which are not offenses against property. Violations of 18 U.S.C. § 2319A (bootlegging) committed prior to passage of § 2323 may fall into this category. Defendants can argue that those crimes are not offenses against property on the ground that bootleg music and music video recordings do not infringe copyrighted property, see Section F. of Chapter II of this Manual, or any other type of property, and that any

revenues from these offenses do not represent an actual pecuniary harm to the victim because bootleg music and music video recordings do not decrease artists' sales. Prosecutors may wish to consult CCIPS at (202) 514-1026 to discuss restitution in § 2319A convictions for offenses committed prior to October 13, 2008.

Fortunately, even for intellectual property offenses committed before passage of § 2323 and not covered by the mandatory restitution provisions, there are other mechanisms to obtain restitution. First, restitution can always be made part of a plea agreement. *See* 18 U.S.C. § 3663(a)(3). Second, a court can order discretionary restitution in any intellectual property criminal case as a condition of probation or of supervised release after imprisonment. *See* 18 U.S.C. §§ 3563(b)(2) (probation), 3583(d) (supervised release). A good example of these principles is *United States v. Lexington Wholesale Co.*, 71 Fed. Appx. 507 (6th Cir. 2003), in which a defendant was convicted for selling infant formula repackaged with counterfeit trademarks and without an accurate "use by" date, which resulted in one count for criminal trademark violations under 18 U.S.C. § 2320 and one count for misbranded food or drugs under Title 21. 71 Fed. Appx. at 508. The sentencing court imposed restitution to the victim of the misbranding count only, which the defendant argued was improper because restitution is authorized only for offenses under Title 18, not Title 21. *Id.* The appellate court affirmed restitution on the ground that it was authorized as a condition of probation and also by the plea agreement. *Id.* at 508-09. Finally, restitution is available for pre-PRO-IP Act violations of 18 U.S.C. § 2319A under the discretionary provisions of 18 U.S.C. § 3663(a)(1)(A), which do not limit restitution to offenses against property.

In deciding whether to award discretionary restitution, the court must consider not only the victim's loss, but also the defendant's financial resources. 18 U.S.C. § 3663(a)(1)(B)(i); *see also* § 3563(b)(2) (allowing court to order restitution to a victim as a condition of probation "as [] reasonably necessary" and without regard to the limitations on restitution in § 3663(a) and § 3663A(c)(1)(A)). Mandatory restitution requires full restitution. *Prosecutor's Guide to Criminal Monetary Penalties* at 29-30. There is, however, a presumption for full restitution, even in discretionary restitution cases. *Id.* The Department's policy is to require full restitution in discretionary cases (assuming the defendant's current or future economic circumstances warrant it), but in discretionary cases to require nominal payment if economic circumstances so warrant. *Id.* at 30.

With respect to awarding discretionary restitution, the court should also consider whether "the complication and prolongation of the sentencing process ... outweighs the need to provide restitution." 18 U.S.C. § 3663(a)(1)(B)(ii). Again, however, the Department advises that "prosecutors should only ask the court to apply this provision narrowly, i.e., only to whatever portion of restitution it may be applicable, and to impose restitution for those victims and harms the court can identify." *Prosecutor's Guide to Criminal Monetary Penalties* at 30.

Department policy requires consideration of the availability of restitution when making charging decisions, and to structure plea agreements to provide restitution whenever possible. *See* U.S. Dep't of Justice, *Attorney General Guidelines for Victim and Witness Assistance*, Art. V, H.1.b (2012) (stating that "[w]hen exercising their discretion, prosecutors should give due consideration to the need to provide full restitution to the victims of federal criminal offenses," among other charging considerations), V, H.1.d (stating that "[w]hen reasonably possible, plea agreements should identify victims' losses for purposes of restitution and address the manner of payment"). If one of the charges would require restitution, the plea agreement should require full restitution even if the defendant pleads guilty to a charge that would not require restitution. *Id.* (citing USAM 9-16.320).

2. Identifying Victims Who Qualify for Restitution

Prosecutors should consider all victims who suffered a loss, from the intellectual property rights-holder, to distributors, and to the direct purchaser and ultimate consumer of the infringing good.

Generally, the intellectual property rights-holder whose works were infringed or misappropriated qualifies for restitution. This is clear in cases involving copyrights, trademarks, and trade secrets. As noted in Section D.1. of this Chapter, however, DMCA offenses do not qualify for mandatory restitution. The court, of course, may still order discretionary restitution. *See United States v. Whitehead*, 532 F.3d 991, 993 (9th Cir. 2008) (in a DMCA case, finding reasonable a sentence including restitution). Moreover, the company whose technological measures are circumvented may be entitled to restitution if the company also owns copyrighted works that were infringed as a result of the circumvention. *United States v. Oliver*, No. 8:02CR3, 2005 WL 1691049, at *5 (D. Neb. July 18, 2005) ("Even if Sony had made money as a result of the defendant's criminal conduct [in modifying Sony Playstations to play pirated

games in violation of the DMCA], it simply does not negate the fact that the defendant is guilty of violating Sony's copyright [by modifying the game machines to play pirated Sony games]."). Similarly, satellite service providers may be eligible for restitution from the sellers of circumvention devices for the amount customers would have paid for the extra channels they obtained fraudulently. *See Brereton*, 196 Fed. Appx. at 693 (affirming restitution order based on loss to DIRECTV of payments from top customers who purchased illicit access cards from defendant); *United States v. Manzer*, 69 F.3d 222, 230 (8th Cir. 1995) (affirming restitution order for defendant who sold modified TV descrambling devices even though he was not actually convicted of a violation of 47 U.S.C. § 605(e)(3)(C)(i)(II) because this was nevertheless part of his scheme to defraud underlying his wire fraud conviction); *United States v. Hicks*, 46 F.3d 1128, 1995 WL 20791, at *1 (4th Cir. Jan. 20, 1995) (table) (holding that defendant convicted of selling modified satellite TV descrambling devices in violation of 47 U.S.C. § 605(e)(4) was not liable for restitution to descrambling device manufacturers because they had been fully compensated when they originally sold their devices, but ordering restitution to satellite service providers for what customers would have paid for the additional channels they could receive because of the defendant's modifications). Industry associations that represent intellectual property rights holders can, in some circumstances, help identify rights holders and receive and distribute the restitution to the rights holders. For a listing of industry contacts, see Appendix G or contact CCIPS at (202) 514-1026.

At least one court has held that a distributor, in addition to the rights holders, may qualify for restitution. In *United States v. Chalupnik*, 514 F.3d 748 (8th Cir. 2008), the court found that BMG Columbia House, which sells copyrighted CDs and DVDs, was a victim for purposes of restitution, but ultimately declined to order restitution because BMG could not prove lost sales from defendant's scheme to sell discarded BMG discs to used record stores. *Id.* at 753-54. See Section D.3. of this Chapter.

Defrauded purchasers—if any—are entitled to restitution as well. *See, e.g., United States v. Trevino*, 956 F.2d 276, 1992 WL 39028 (9th Cir. 1992) (table) (in counterfeit trademark prosecution, affirming order of restitution to nuclear power plant victim that had purchased counterfeit circuit breakers). A defendant who has defrauded a large number of consumers can be expected to argue that restitution is not required because the class of defrauded consumers is impracticably large or difficult to identify. *See* 18 U.S.C. § 3663A(c)(3).

There are procedures for ordering restitution for victims who can be identified by name but cannot presently be located at a particular address. *See United States v. Berardini*, 112 F.3d 606, 609-12 (2d Cir. 1997).

Consumers who knew that they were purchasing counterfeits generally do not qualify as victims, because they have not been harmed. Distinguishing between consumers who were and were not defrauded may be a challenge.

In determining whether an involved party qualifies as a victim for the purpose of restitution, the court will distinguish between those harmed by the defendant's relevant conduct and those harmed by the offense of conviction. (The rest of this paragraph consists largely of excerpts from the *Prosecutor's Guide to Criminal Monetary Penalties* at 32, with minor edits.) The court is statutorily authorized to impose restitution only to identifiable victims of the acts that are part of the offense of conviction. In *Hughey v. United States*, 495 U.S. 411, 413 (1990), the Supreme Court held that the restitution statutes limit restitution to "the loss caused by the specific conduct that is the basis of the offense of conviction." Restitution is not authorized for acts merely related to the offense of conviction, such as acts that are within "relevant conduct" under guideline sentencing (U.S.S.G. § 1B1.3), but are outside the actual offense of conviction itself. Under the primary restitution statutes, amended after the *Hughey* decision, a victim is "a person directly and proximately harmed as a result of the commission of an offense for which restitution may be ordered." 18 U.S.C. §§ 3663A(a)(2), 3663(a)(2). This includes, in a case where the offense of conviction includes a scheme, conspiracy, or pattern of criminal activity, "any person directly harmed by the defendant's criminal conduct in the course of the scheme, conspiracy, or pattern" of criminal activity. *Id*. Therefore, prosecutors should charge such offenses to indicate the specific nature and full extent of the acts that constitute the scheme, conspiracy, or pattern of which the offense of conviction is involved, in order to permit the broadest imposition of restitution.

If the acts for which restitution is sought are outside the offense of conviction and cannot be otherwise tied to a scheme, pattern, or conspiracy that is an element of the offense of conviction, then restitution is unavailable. Under this rule, restitution is generally not triggered by one kind of act if the offense of conviction describes another kind of act, even if the acts are logically related in purpose or intent. *See, e.g., United States v. Blake*, 81 F.3d 498 (4th Cir. 1996) (court denied restitution to victims for use of stolen credit cards where offense of conviction was possession of stolen credit cards); *United States*

v. Hayes, 32 F.3d 171 (5th Cir. 1994); *cf. In re Doe*, 264 Fed. Appx. 260, 263-64 (4th Cir. 2007) (court denied restitution to petitioner seeking restitution for addiction to prescription pain medication from defendant pharmaceutical company's misbranding offense where she provided no evidence that she relied on any false or misleading information).

Other courts apply this rule less strictly. For example, to determine the existence of a scheme and what acts it included for purposes of restitution, some courts will consider the facts alleged in the indictment, proven at trial, or admitted in the plea colloquy. *See, e.g., United States v. Ramirez*, 196 F.3d 895 (8th Cir. 1999); *United States v. Jackson*, 155 F.3d 942 (8th Cir. 1998); *United States v. Hughey*, 147 F.3d 423, 438 (5th Cir. 1998) (suggesting that restitution might have been triggered by acts not in the indictment had they been established by the trial record)

If no scheme, conspiracy, or pattern encompasses the acts for which injured parties seek restitution, restitution will likely be limited in two respects. First, a party who was injured solely by an act outside the offense of conviction—such as a party whose losses were proved only as relevant conduct—cannot obtain restitution. Second, a party who was injured by the offense of conviction can obtain restitution only for the offense-of-conviction acts and not acts proved only as relevant conduct at sentencing—even relevant conduct that counted towards the loss or infringement amount; however, some courts may still allow restitution for this type of relevant conduct if it is alleged in the indictment or proved at trial, not just at sentencing. The exception to both these limitations is, of course, restitution ordered pursuant to a stipulation in a plea agreement. *See* 18 U.S.C. § 3663(a)(3).

Application of these principles to an intellectual property crime occurred in *United States v. Manzer*, 69 F.3d 222 (8th Cir. 1995), in which the court ordered $2.7 million in restitution from a defendant convicted of mail fraud, wire fraud, and criminal copyright infringement for trafficking in cloned computer chips. The cloned chips would allow satellite descrambling devices to decrypt cable satellite signals without authorization. The defendant objected to the $2.7 million restitution award on the ground that it included sales not identified in the indictment. *Id.* at 229-30. The Eighth Circuit disagreed, holding that the mail and wire fraud counts alleged a scheme to defraud that "encompass[ed] transactions beyond those alleged in the counts of conviction," including the sales not otherwise identified in the indictment. *Id.* at 230 (citation and internal quotation marks omitted). Note that the restitution

might have been limited to the sales alleged in the indictment if the defendant had pleaded to or been convicted of only the copyright charge.

There are several ways to help ensure that restitution is awarded for harm caused. As part of any plea deal, the government should require the defendant to plead to the counts that offer maximum restitution, or the government should insist upon a comprehensive plea agreement that provides restitution to the victims of relevant offense conduct (whether the statutes or offenses of conviction provide for it or not). *See* 18 U.S.C. § 3663(a)(3) (allowing court to order restitution as provided in plea agreement); *Prosecutor's Guide to Criminal Monetary Penalties* at 22-24.

At the beginning of the case, prosecutors should draft the indictment to maximize restitution. *Id*. at 21. As the *Prosecutor's Guide to Criminal Monetary Penalties* counsels:

> Prosecutors should avoid the "scheme" restitution pitfalls by:
>
> a) Charging offenses that involve the statutory elements of an "intent to defraud" or "intent to deceive" in the traditional wire/mail fraud (or conspiracy) format, where the scheme (or conspiracy) is described in detail and incorporated by reference into each specific act count; and
>
> b) Making sure the dates alleged as the beginning and end of the scheme or conspiracy include all acts in furtherance of the scheme or conspiracy for which restitution should be imposed.

Id. at 22. Moreover, "[s]imply tracking the statutory language of such offenses does not clarify if the acts of conviction are part of a scheme, i.e., whether different kinds of acts make up a scheme to 'defraud' or 'deceive.' Numerous restitution orders have been vacated in such cases due to ambiguity of the 'scheme' issue." *Id*. The same concerns apply to whether acts in addition to those alleged as overt acts of a conspiracy can qualify as part of the conspiracy for purposes of awarding restitution. The *Prosecutor's Guide to Criminal Monetary Penalties* discusses specific ways to structure restitution provisions in a plea agreement to maximize restitution. *Id*. at 23-24.

3. Determining a Restitution Figure

Once the government has identified the people and entities who might be classified as victims—consumers who were defrauded and intellectual property

rights holders—the next question is how to calculate what the victims are owed, if anything.

To begin with, as discussed in the prior section, the restitution award must be based on the loss caused by the defendant's offense of conviction.

After determining which victims and transactions qualify for restitution, the government must determine how the restitution should be calculated. The most important principle is that restitution is intended to make the victims whole by compensating them for their losses. *See* 18 U.S.C. §§ 3663(a)(1)(B)(i)(I), 3663A(b), 3664(a); U.S.S.G. § 5E1.1(a). This principle has several consequences.

First, the restitution order should require the defendant to return any of the victim's property that he took. *See* 18 U.S.C. §§ 3663(b)(1)(A), 3663A(b)(1)(A), 3664(f)(4)(A). This principle applies across all intellectual property offenses:

- In trade secret offenses, the defendant should be required to return the trade secret and any other items that he took from the owner of the trade secret.
- In infringement cases, the defendant should be required to return the money he accepted from the customers he defrauded (if any—in some cases the customers knew that they were receiving counterfeits). Although the defendant might argue that he is entitled to offset the value of the goods the defrauded customers received, often that value is next to nothing. *Compare United States v. West Coast Aluminum Heat Treating Co.*, 265 F.3d 986, 992 (9th Cir. 2001) ("And, by reducing the loss calculation to account for the partial benefit gained by the government, the district court remained consistent with the rule that the victim's loss should be offset by the victim's benefit."), *and United States v. Matsumaru*, 244 F.3d 1092, 1109 (9th Cir. 2001) (holding that restitution of the purchase price for the business the victim paid for and was promised but did not receive, must be offset by the value of the van and business license he did receive), *with United States v. Angelica*, 859 F.2d 1390, 1394 (9th Cir. 1988) (affirming trial court's refusal to offset restitution award by value of substitute property given to victims, because there was "no abuse of discretion in the district court's decision to disregard the value of the inexpensive garnets that were unwanted by the victims and substituted for their diamonds as part of the fraudulent scheme"), *and United States v. Austin*, 54 F.3d 394, 402 (7th Cir. 1995)

(holding that "even if the [counterfeit or misrepresented art] pieces Austin sold ... were not completely worthless, $0 was the best estimate of their worth" for purposes of calculating loss).

- In infringement cases—and perhaps trade secret cases as well—the defendant should also compensate the intellectual property rights-holder victims for any sales that he diverted from them. *See United States v. Milstein*, 481 F.3d 132, 136-37 (2d Cir. 2007) (finding, in criminal trademark prosecution, that restitution should be based on the rights holders' "lost sales," as provided in the civil trademark provisions of the Lanham Act, 15 U.S.C. § 1117(a)(1)-(2); those sales represented the "value of the property" cited in the Victim and Witness Protection Act of 2008, 18 U.S.C. § 3663(b)(1)(B)); *United States v. Sung*, 51 F.3d 92, 94 (7th Cir. 1995) (holding, in criminal trademark prosecution, that "[r]estitution in a criminal case is the counterpart to damages in civil litigation"). If the defendant's conduct did not divert any sales from the victim, then the victim may not be entitled to restitution. *See United States v. Chalupnik*, 514 F.3d 748, 755 (8th Cir. 2008) (reversing restitution order because victim offered only speculation as to lost sales); *United States v. Hudson*, 483 F.3d 707, 710-11 (10th Cir. 2007) (reversing restitution order because no evidence that victim Microsoft suffered lost sales as result of defendant's conduct); *United States v. Foote*, No. CR.A. 00-20091-01-KHV, 2003 WL 22466158, at *7 (D. Kan. July 31, 2003) (refusing to award restitution to trademark-holders because the government proposed no reliable estimate of the victim's losses and citing cases for the need to prove lost profits). A defendant is most likely to divert sales from the victim when he has defrauded customers into thinking that his product or service is authentic, although he may have a counter-argument if his prices were sufficiently under the authentic price that his customers would have been unlikely to pay the victim the full price for the real thing. A consumer who pays $20 for a high-quality (or even a low-quality) fake purse might not have paid full price ($120 to $700) for the real purse, and thus his purchase of the fake might not represent a lost sale to the victim. Similarly, some computer users who download a $60,000 engineering program for free from an infringing website or peer-to-peer network may be "trophy hunters" who would not have paid full price for an authorized copy, whereas other downloaders may be businesspeople who would have paid full price had the free download not been available. Restitution orders

should differentiate between these situations, to the extent possible. Prosecutors might also try to introduce evidence establishing that the availability of high-quality infringing works affected the market for the victim's product. *See Brooktree Corp. v. Advanced Micro Devices, Inc.*, 977 F.2d 1555, 1579 (Fed. Cir. 1992) (civil case upholding "actual damages" calculation based on evidence that plaintiff had been forced to lower its prices as a result of defendant's infringing activities).

- Restitution based on lost sales is generally not calculated by the defendant's gain, but rather by the victim's loss. *Foote*, 2003 WL 22466158, at *7. For example, in *United States v. Martin*, 64 Fed. Appx. 129 (10th Cir. 2003), the total value of the items infringed was $1,143,395, but the restitution equaled only $395,000—the retail value multiplied by the rights-holder's profit margin. As Martin illustrates, restitution is based on lost net profits, not on total retail price. *See United States v. Beydoun*, 469 F.3d 102, 108 (5th Cir. 2006). Nevertheless, the defendant has no right to have his own costs offset against his gain. *United States v. Chay*, 281 F.3d 682, 686-87 (7th Cir. 2002).
- When the evidence of infringement consists of the defendant's inventory of infringing product rather than his actual sales—and the defendant therefore argues against any restitution for lack of actual diverted sales—the government may argue that the inventory is a reasonable estimate of the defendant's past sales. This argument is likely to be most persuasive when the defendant's inventory is counted after he has been in business for a long time. Inventory is more likely to overstate past sales when a business is just starting out, and to understate past sales when the business has been successful and ongoing for a substantial time.
- At least one court has held that restitution in a criminal intellectual property case can be based on the amount of statutory damages that the victim could have obtained from the defendant in a civil case, but this was a case in which the statutory damages likely understated the actual damages. *See United States v. Manzer*, 69 F.3d 222, 229-30 (8th Cir. 1995) (upholding restitution award in descrambler case of $2.7 million for 270 cloning devices based on minimum statutory damages of $10,000 per device, where victim provided loss figure of over $6.8 million). Statutory damages are available in civil suits for a variety of intellectual property violations. *See, e.g.*, 15 U.S.C. § 1117(c) (statutory

damages of $1,000-$200,000 (up to $2 million if infringement was willful) per counterfeit mark per type of goods or services); 17 U.S.C. § 504(c) (statutory damages of $750-$30,000 (up to $150,000 if infringement was willful) per infringed work); 47 U.S.C. § 605(e)(3)(C)(i)(II) (statutory damages of $10,000-$100,000 per violation). *See also* Roger D. Blair & Thomas F. Cotter, *An Economic Analysis of Damages Rules in Intellectual Property Law*, 39 Wm. & Mary L. Rev. 1585, 1651-72 (1998) (discussing economic theory of statutory damages in copyright law).

- If the defendant earned a profit from his crime but the court finds that restitution is too difficult to calculate, the court can nevertheless take away the defendant's gain by imposing a fine in the amount of his gain. *See Foote*, 2003 WL 22466158, at *7.

Second, the restitution order should compensate the victim for any money spent to investigate the defendant's conduct, whether during the victim's own investigation or while helping the government investigate and prosecute. These costs often arise in intellectual property cases: employers conduct internal investigations into their employees' theft of trade secrets, and copyright and trademark-holders often hire private investigators to monitor and investigate suspected infringers. The mandatory and discretionary restitution statutes both authorize restitution "for lost income and necessary child care, transportation, and other expenses [related to / incurred during] participation in the investigation or prosecution of the offense or attendance at proceedings related to the offense." 18 U.S.C. §§ 3663(b)(4), 3663A(b)(4). These provisions have been interpreted to cover not only the victim's expenses in helping the government, but also the costs of the victim's own investigation. *See United States v. Brown*, 150 Fed. Appx. 575 (8th Cir. 2005) (per curiam) (awarding restitution to victim company for staff investigation costs into reconstructing and correcting financial records related to defendant's embezzlement, where defendant contested proof of amount but not whether investigative costs as a category are awardable); *United States v. Beaird*, 145 Fed. Appx. 853 (5th Cir. 2005) (per curiam) (affirming $200,000 award of restitution for attorney's fees and litigation expenses associated with assisting the FBI's investigation); *United States v. Gordon*, 393 F.3d 1044, 1049, 1056-57 (9th Cir. 2004) (discussing reimbursement of investigative costs in depth, in case affirming $1,038,477 in restitution for costs of company's internal investigation and responses to grand jury subpoenas), *cert. denied*, 126 S. Ct. 472 (2005); *see also United States v. Susel*, 429 F.3d 782, 784 (8th Cir. 2005) (per curiam) (affirming award

of software company's administrative and transportation expenses during participation in the investigation and prosecution of the offense in criminal copyright case). *But see United States v. Saad*, 544 F. Supp. 2d 589, 592 (E.D. Mich. 2008) (denying restitution for investigative and legal costs incurred by victim who pursued civil litigation arising from defendant's criminal conduct).

Third, as explained above in Section D.1. of this Chapter, in deciding whether to award discretionary restitution, the court must consider not only the victim's loss, but also the defendant's financial resources. 18 U.S.C. § 3663(a)(1)(B)(i). A presumption for full restitution exists even in discretionary restitution cases. *Prosecutor's Guide to Criminal Monetary Penalties* at 29-30. Unless economic circumstances warrant nominal payment, Department policy requires full restitution in discretionary cases. *Id.* at 30. In no case shall the fact that a victim has received or is entitled to receive compensation with respect to a loss from insurance or any other source be considered in determining the amount of restitution. 18 U.S.C. § 3664(f)(1)(B).

Fourth, victims have an important role in helping to determine the appropriate amount of restitution. The government must consult with witnesses and the court to consider victims' evidence at sentencing. *See* 42 U.S.C. § 10607(c)(3)(G); U.S. Dep't of Justice, *Attorney General Guidelines for Victim and Witness Assistance*, Art. IV, I.2 (2012). See generally Chapter X of this Manual (Victims). The criminal intellectual property statutes similarly require the court to consider victims' evidence at sentencing. *See* 18 U.S.C. §§ 2319(d), 2319A(d), 2319B(e), 2320(e). The pre-sentence report must also include a verified assessment of victim impact in every case. Fed. R. Crim. P. 32(d)(2)(B). Trade associations can be very helpful in providing victim impact statements, particularly when an offense involves a large quantity and variety of infringing products. See the listing of intellectual property contacts in Appendix G of this Manual.

E. Forfeiture

In criminal intellectual property cases, forfeiture can serve several important functions. Forfeiting infringing items removes them from the stream of commerce so they cannot be sold or redistributed. Forfeiting the tools and equipment that defendants use to commit intellectual property crimes—ranging from manufacturing equipment to computers to domain names used by infringing websites—prevents their use to commit further IP

crime. Forfeiting the proceeds of intellectual property crime—the revenues and profits—prevents their reinvestment in a criminal enterprise. Finally, forfeiture can serve as a powerful deterrent.

For IP offenses committed on or after October 13, 2008, forfeiture is fairly straightforward. The Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008 created a new section, 18 U.S.C. § 2323, which expressly authorizes forfeiture for intellectual property offenses:

> (a) Civil forfeiture.
>
> (1) Property subject to forfeiture. The following property is subject to forfeiture to the United States Government:
>
> (A) Any article, the making or trafficking of which is, prohibited under section 506 of title 17, or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of this title.
>
> (B) Any property used, or intended to be used, in any manner or part to commit or facilitate the commission of an offense referred to in subparagraph (A).
>
> (C) Any property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of an offense referred to in subparagraph (A).
>
> (2) Procedures. The provisions of chapter 46 relating to civil forfeitures shall extend to any seizure or civil forfeiture under this section. For seizures made under this section, the court shall enter an appropriate protective order with respect to discovery and use of any records or information that has been seized. The protective order shall provide for appropriate procedures to ensure that confidential, private, proprietary, or privileged information contained in such records is not improperly disclosed or used. At the conclusion of the forfeiture proceedings, unless otherwise requested by an agency of the United States, the court shall order that any property forfeited under paragraph (1) be destroyed, or otherwise disposed of according to law.
>
> (b) Criminal forfeiture.

(1) Property subject to forfeiture. The court, in imposing sentence on a person convicted of an offense under section 506 of title 17, or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of this title, shall order, in addition to any other sentence imposed, that the person forfeit to the United States Government any property subject to forfeiture under subsection (a) for that offense.

(2) Procedures.

(A) In general. The forfeiture of property under paragraph (1), including any seizure and disposition of the property and any related judicial or administrative proceeding, shall be governed by the procedures set forth in section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), other than subsection (d) of that section.

(B) Destruction. At the conclusion of the forfeiture proceedings, the court, unless otherwise requested by an agency of the United States shall order that any--

(i) forfeited article or component of an article bearing or consisting of a counterfeit mark be destroyed or otherwise disposed of according to law; and

(ii) infringing items or other property described in subsection (a)(1)(A) and forfeited under paragraph (1) of this subsection be destroyed or otherwise disposed of according to law.

PRO-IP Act of 2008, Pub. L. No. 110-403, § 206, 122 Stat. 4256, 4262-63 (2008); 18 U.S.C. § 2323. Notably, the PRO-IP Act makes criminal forfeiture mandatory for all offenses covered by the act. *See* 18 U.S.C. § 2323(b)(1).

For intellectual property offenses committed prior to passage of the PRO-IP Act, forfeiture is governed by a complex web of forfeiture statutes. This Chapter is not a definitive guide to forfeiture law, but rather it provides a basic overview of the forfeiture remedies available in IP crimes. Prosecutors with questions concerning forfeiture practice and procedure should contact the forfeiture expert in their office or the Criminal Division's Asset Forfeiture and Money Laundering Section at (202) 514-1263.

1. Property Subject to Forfeiture

Intellectual property crimes give rise to three general categories of forfeitable property:

1) Contraband items, which include infringing copyrighted copies and phonorecords; goods, labels, documentation, and packaging that bear counterfeit trademarks, service marks, or certification marks; and unauthorized recordings of live musical performances. *See* 49 U.S.C. § 80302(a)(6) (defining "contraband"). These items are subject to forfeiture under the PRO-IP Act, see 18 U.S.C. § 2323(a)(1)(A), and they were generally forfeitable prior to its enactment on October 13, 2008. *See, e.g.*, 18 U.S.C. § 2320(b)(3)(A)(iii).

2) Proceeds derived from the commission of an IP offense. These are subject to forfeiture under the PRO-IP Act, *see* 18 U.S.C. § 2323(a)(1)(C), and they were usually forfeitable prior to its enactment. *See, e.g.*, 18 U.S.C. § 1834(a)(1) (effective October 11, 1996 through October 12, 2008); 18 U.S.C. 2320(b)(3)(A)(i) (effective March 16, 2006 through October 12, 2008).

3) Facilitating property, that is, property that was used to commit or facilitate the IP offense, such as plates, molds or masters used to produce copyright-infringing works; computers, tools, equipment, and supplies used to produce counterfeit goods; and vehicles used to traffic in any of the above. Such property is subject to forfeiture under the PRO-IP Act, *see* 18 U.S.C. § 2323(a)(1)(B); prior to the act's passage, forfeiture of facilitating property was available in many cases, but its availability varied substantially depending on the specific IP offense, the type of property, and the type of forfeiture sought; *see, e.g.*, 18 U.S.C. § 1834(a)(2) (effective October 11, 1996 through October 12, 2008); 18 U.S.C. 2320(b)(3)(A)(ii) (effective March 16, 2006 through October 12, 2008).

2. Overview of Forfeiture Procedures

There are three types of forfeiture procedures: administrative, civil, and criminal. This section gives a brief overview and includes a table that

summarizes the types of forfeiture available for each kind of property, organized by intellectual property offense.

a. Administrative Forfeiture Proceedings

Administrative forfeiture occurs when a law enforcement agency forfeits property in an administrative, non-judicial matter. As with the other types of forfeiture procedure, administrative forfeiture is available only pursuant to a specific statute that authorizes such a procedure. Administrative forfeiture commences once an agency seizes property and then sends or publishes notice of the property seizure within the prescribed deadlines. If nobody responds to the notice by filing a claim of ownership claim within the allotted time, the property is forfeited without involving a prosecutor or judge. If a claim is filed, the seizing agency must either return the property or seek forfeiture through a judicial procedure.

With the passage of the PRO-IP Act on October 13, 2008, administrative forfeiture is now available for all IP offenses except violations of the DMCA. *See* 18 U.S.C. § 2323(a)(2). Administrative forfeiture is also available for some IP offenses under several other statutes, including: 17 U.S.C. § 603(c) (copyright-infringing imports and exports); 19 U.S.C. § 1526(e) (trademark-infringing imports); 18 U.S.C. § 981(d) and 19 U.S.C. §§ 1607-09 (proceeds); 49 U.S.C. § 80304 (facilitating property).

Real property and personal property (other than monetary instruments) that are worth more than $500,000 can never be forfeited in an administrative proceeding. *See* 19 U.S.C. § 1607; 18 U.S.C. § 985.

b. Civil and Criminal Proceedings

Unlike administrative forfeiture proceedings, civil and criminal forfeiture are judicial actions that require the involvement of prosecutors and the courts.

Criminal forfeiture is an *in personam* proceeding that begins with a forfeiture allegation in an indictment and is then executed as part of a defendant's sentence. It thus requires a conviction and is limited to property belonging to the defendant that was involved in the offense of conviction. Criminal forfeiture cannot reach a third-party's property, even if the defendant used the third-party's property to commit the crime.

Whereas criminal forfeiture is an *in personam* action against the defendant, civil forfeiture is an in rem action against the property itself. This means that

civil forfeiture proceedings can reach property regardless of who owns it, if the government can prove that the property was derived from or used to commit a crime. Civil forfeiture proceedings are not part of a criminal case at all. The burden of proof is a preponderance of the evidence, and civil forfeiture proceedings can dispose of property even without a criminal conviction or the filing of any criminal charges.

c. Table of Forfeiture Provisions Arranged by Criminal IP Statute

The following table indicates the types of forfeiture available for intellectual property offenses committed since passage of the PRO-IP Act on October 13, 2008. For a listing of the types of forfeiture available prior to that, see Appendix I. Note that administrative forfeiture is generally available for vessels used to transport contraband items pursuant to 49 U.S.C. § 80304. Note also that even where forfeiture of proceeds from intellectual property offenses is not provided for expressly, it may be available indirectly through money laundering statutes.

Criminal Copyright Infringement

Administrative	
Infringing Items	**Yes.** • 17 U.S.C. §§ 602-603 (prohibiting imports and exports of infringing copies). • 18 U.S.C. § 2323(a)(2) (permitting administrative forfeiture of infringing items forfeitable civilly). • 19 U.S.C. §§ 1595a, 1607-09 (forfeiture & seizure by CBP of infringing items).
Facilitating Property	**Yes.** • 18 U.S.C. § 2323(a)(2) (permitting administrative forfeiture of facilitating property forfeitable civilly). • 19 U.S.C. §§ 1595a, 1607-09 (forfeiture & seizure by CBP).
Proceeds	**Yes.** • 18 U.S.C. § 981(d) (permitting administrative forfeiture of proceeds forfeitable civilly). • 18 U.S.C. § 2323(a)(2) (same).

Civil	
Infringing Items	**Yes**. • 17 U.S.C. §§ 602-603. • 18 U.S.C. § 2323(a)(1)(A).
Facilitating Property	**Yes.** • 18 U.S.C. § 2323(a)(1)(B).
Proceeds	**Yes.** • 18 U.S.C. §§ 981(a)(1)(C) & 2323(a)(1)(C).
Criminal	
Infringing Items	**Yes (mandatory) .** • 17 U.S.C. §§ 602-603. • 18 U.S.C. § 2323(b)(1) (*mandating* criminal forfeiture of property forfeitable civilly). • 28 U.S.C. § 2461(c) (*permitting* criminal forfeiture of property forfeitable civilly).
Facilitating Property	**Yes (mandatory)**. • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).
Proceeds	**Yes (mandatory).** • 18 U.S.C. § 981(a)(1)(C). • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).

Digital Millennium Copyright Act

Administrative	**No.**
Civil	**No.**
Criminal	**No**.

Economic Espionage Act (Trade Secret Theft)

Administrative	
Contraband	**Yes.** • 18 U.S.C. § 2323(a)(2).
Facilitating Property	**Yes.** • 18 U.S.C. § 2323(a)(2).
Proceeds	**Yes.** • 18 U.S.C. § 2323(a)(2).
Civil	
Contraband	**Yes.** • 18 U.S.C. § 2323(a)(1)(A).
Facilitating Property	**Yes.** • 18 U.S.C. § 2323(a)(1)(B).
Proceeds	**Yes.** • 18 U.S.C. § 2323(a)(1)(C).
Criminal	
Contraband	**Yes (mandatory)**. • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).
Facilitating Property	**Yes (mandatory).** • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).
Proceeds	**Yes (mandatory).** • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).

Counterfeit/Illicit Labels, Documentation, and Packaging for Copyrighted Works

Administrative	
Counterfeit/Infringing Items	**Yes.** • 18 U.S.C. § 2323(a)(2). • 19 U.S.C. §§ 1595a, 1607-09.
Facilitating Property	**Yes.** • 18 U.S.C. § 2323(a)(2). • 19 U.S.C. §§ 1595a, 1607-09.
Proceeds	**Yes.** • 18 U.S.C. § 2323(a)(2).

Civil	
Counterfeit/Infringing Items	**Yes**. • 18 U.S.C. § 2323(a)(1)(A).
Facilitating Property	**Yes.** • 18 U.S.C. § 2323(a)(1)(B).
Proceeds	**Yes.** • 18 U.S.C. § 981(a)(1)(C). • 18 U.S.C. § 2323(a)(1)(B).
Criminal	
Counterfeit/Infringing Items	**Yes (mandatory)**. • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).
Facilitating Property	**Yes (mandatory).** • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).
Proceeds	**Yes (mandatory).** • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).

Unauthorized Fixations of Live Musical Performances ("Bootlegging")

Administrative	
Unauthorized Recordings	**Yes.** • 18 U.S.C. § 2319A(c). • 18 U.S.C. § 2323(a)(2). • 19 U.S.C. § 1595a, 1607-09.
Facilitating Property	**Yes.** • 18 U.S.C. § 2323(a)(2). • 19 U.S.C. § 1595a, 1607-09.
Proceeds	**Yes.** • 18 U.S.C. § 2323(a)(2).
Civil	
Unauthorized Recordings	**Yes.** • 18 U.S.C. § 2319A(c). • 18 U.S.C. § 2323(a)(1)(A).
Facilitating Property	**Yes.** • 18 U.S.C. § 2323(a)(1)(B).
Proceeds	**Yes.** • 18 U.S.C. § 981(a)(1)(C). • 18 U.S.C. § 2323(a)(1)(C).

Criminal	
Unauthorized Recordings	**Yes (mandatory)**. • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).
Facilitating Property	**Yes (mandatory).** • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).
Proceeds	**Yes (mandatory).** • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).

Unauthorized Recording of Motion Pictures ("Camcording")

Administrative	
Unauthorized Recordings	**Yes.** • 18 U.S.C. § 2323(a)(2). • 19 U.S.C. § 1595a, 1607-09.
Facilitating Property	**Yes.** • 18 U.S.C. § 2323(a)(2). • 19 U.S.C. § 1595a, 1607-09.
Proceeds	**Yes.** • 18 U.S.C. § 2323(a)(2).
Civil	
Unauthorized Recordings	**Yes.** • 18 U.S.C. § 2323(a)(1)(A).
Facilitating Property	**Yes.** • 18 U.S.C. § 2323(a)(1)(B).
Proceeds	**Yes.** • 18 U.S.C. § 2323(a)(1)(C).
Criminal	
Unauthorized Recordings	**Yes (mandatory).** • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).
Facilitating Property	**Yes (mandatory).** • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).
Proceeds	**Yes (mandatory).** • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).

Goods, Services, Labels, Documentation, and Packaging with Counterfeit Marks

Administrative	
Counterfeit Items	**Yes.** • 18 U.S.C. § 2323(a)(2). • 19 U.S.C. § 1526(e). • 19 U.S.C. §§ 1595a & 1607-09.
Facilitating Property	**Yes.** • 18 U.S.C. § 2323(a)(2). • 19 U.S.C. §§ 1595a & 1607-09.
Proceeds	**Yes.** • 18 U.S.C. § 981(d). • 18 U.S.C. § 2323(a)(2).
Civil	
Contraband	**Yes.** • 18 U.S.C. § 2323(a)(1)(A).
Facilitating Property	**Yes.** • 18 U.S.C. § 2323(a)(1)(B).
Proceeds	**Yes.** • 18 U.S.C. § 981(a)(1)(C). • 18 U.S.C. § 2323(a)(1)(C).
Criminal	
Contraband	**Yes (mandatory)**. • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).
Facilitating Property	**Yes (mandatory).** • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).
Proceeds	**Yes (mandatory).** • 18 U.S.C. § 981(a)(1)(C). • 18 U.S.C. § 2323(b)(1). • 28 U.S.C. § 2461(c).

3. Choosing a Forfeiture Procedure

Although the prosecutor may commence parallel civil and criminal forfeiture cases to keep all avenues of forfeiture open, various factors may affect which procedure is best to pursue:

- Substitute assets. In criminal proceedings, the court can enter a money judgment against the defendant for the property's value or can order the forfeiture of substitute assets if the property has been dissipated or cannot be found.
- Burden of proof. In civil proceedings, the government need only prove that a crime was committed and that the property derived from or facilitated the crime by a preponderance of the evidence. In criminal cases, the government must prove beyond a reasonable doubt that a crime was committed and that the defendant committed the crime, although the nexus between the property and the offense need be proved only by a preponderance of the evidence.
- Criminal conviction as a prerequisite. Civil forfeiture does not require a conviction. This is especially important if the government wants to forfeit the property of fugitives or defendants who have died, or if the government can prove that the property was involved in a crime but cannot prove the wrongdoer's specific identity. Moreover, civil proceedings may be brought against any property derived from either a specific offense or from an illegal course of conduct, and therefore is not limited to property involved in the offense(s) of conviction.
- Ownership of property. Criminal forfeiture reaches property only if it is owned by the defendant, or was at the time of the offense giving rise to the forfeiture. Civil forfeiture should be considered if the prosecutor seeks to forfeit proceeds or facilitation property that the defendant does not own.
- Discovery and disclosure obligations. Civil forfeiture, governed by civil discovery rules, can result in early or unwanted disclosure of information through traditional civil discovery mechanisms such as interrogatories and depositions, and it is subject to stringent deadlines.
- Attorneys' fees. If the government brings an unsuccessful action for civil forfeiture, it may be liable for the owner's attorneys' fees.
- Efficiency. Administrative forfeiture is preferred whenever available—generally, when no one is contesting the forfeiture—as it can dispose of certain forfeiture matters quickly in a non-judicial setting.

4. Civil Forfeiture in Intellectual Property Matters

With the passage of the PRO-IP Act on October 13, 2008, civil forfeiture is now available for all intellectual property offenses except violations of the DMCA. *See* 18 U.S.C. § 2323(a). Again, the government need only prove that the crime was committed; it need not convict a specific defendant of the crime.

a. Proceeds

The government can seek civil forfeiture of the proceeds of all IP offenses except violations of the DMCA. *See* 18 U.S.C. § 2323(a)(1)(C). In addition, the Civil Asset Forfeiture Reform Act of 2000 (CAFRA) amendments to 18 U.S.C. § 981—a general civil forfeiture statute—permit civil forfeiture of the proceeds of certain IP offenses. The CAFRA amendments permit the government to seek civil forfeiture of "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to," among other things, any offense defined as a specified unlawful activity in the money laundering provisions at 18 U.S.C. § 1956(c)(7). 18 U.S.C. § 981(a)(1)(C). Specified unlawful activities include criminal copyright infringement and trademark counterfeiting, 18 U.S.C. § 1956(c)(7)(D) (citing 18 U.S.C. §§ 2319, 2320), as well as any offense listed as racketeering activity in 18 U.S.C. § 1961(1). Section 1961, in turn, lists not only §§ 2319 and 2320 violations, but also violations of 18 U.S.C. § 2318 (counterfeit labels, documentation, and packaging for copyrighted works) and § 2319A (bootleg musical recordings).

b. Infringing Items, Other Contraband, and Facilitating Property

Civil forfeiture of infringing and other contraband items, as well as facilitating property, is available for all IP offenses except violations of the DMCA. *See* 18 U.S.C. §§ 2323(a)(1)(A), (B).

In addition, there are special civil forfeiture provisions applicable to unauthorized fixations imported into the United States, *see* 18 U.S.C. § 2319A (unauthorized fixations of live musical performances), and to infringing copies imported to or exported from the United States. *See* 17 U.S.C. §§ 602-603.

c. Innocent Owner Defense

In most civil forfeiture actions, the innocent owner defense allows an owner to challenge the forfeiture on the ground that he was unaware that the property was being used for an illegal purpose, or took all reasonable steps under the circumstances to stop it. *See United States v. 2001 Honda Accord EX*,

245 F. Supp. 2d 602 (M.D. Pa. 2003) (holding that CAFRA preserved the rule that the burden of proof shifts to the claimant to establish the innocent owner defense); *United States v. 2526 Faxon Avenue*, 145 F. Supp. 2d 942 (W.D. Tenn. 2001) (holding that CAFRA requires the claimant to prove the affirmative innocent owner defense by a preponderance of the evidence). There are some exceptions, however, most notably for importation offenses, and therefore prosecutors may wish to consult with the Department's Asset Forfeiture and Money Laundering Section at (202) 514-1263 if an innocent owner is likely to submit a claim.

d. Victims' Ability to Forfeit Property

Note also that some IP rights holders may obtain certain civil seizures that can complicate the government's criminal prosecution, not to mention its forfeiture proceedings. Mark-holders have an *ex parte* remedy for seizing infringing products and manufacturing equipment. 15 U.S.C. § 1116(d). Mark-holders may also petition the court for seizure orders during a civil action against an infringer under 15 U.S.C. § 1114. Authority for an *ex parte* seizure order is provided at 15 U.S.C. § 1116(d)(1)(A). Mark-holders who seek such an order must give reasonable notice to the United States Attorney for the judicial district in which the order is sought, after which the United States Attorney "may participate in the proceedings arising under such application if such proceedings may affect evidence of an offense against the United States." 15 U.S.C. § 1116(d)(2). The mark-holder's application may be denied "if the court determines that the public interest in a potential prosecution so requires." *Id*. If the mark-holder's application is granted, then the seizure must be made by a federal, state, or local law enforcement officer. *See* 15 U.S.C. § 1116(d)(9).

Similar *ex parte* seizure remedies are available to rights holders in copyright and counterfeit or illicit labels cases. *See* 17 U.S.C. § 503; 18 U.S.C. § 2318(e).

Prosecutors may need to participate in these civil proceedings in order to preserve evidence relevant to an incipient or ongoing criminal case; to contest the issuance of an order; to preserve an ongoing investigation; or to inform the mark-holder of his ability to initiate a parallel civil case to seize, forfeit, and destroy equipment used to manufacture the counterfeit trademark goods.

5. Criminal Forfeiture in IP Matters

As noted above, criminal forfeiture is an *in personam* action, and thus is available only once a defendant has been convicted, and then it is limited to

property belonging to the defendant. *See United States v. Totaro*, 345 F.3d 989, 995 (8th Cir. 2003) (holding that criminal forfeiture is *in personam*, because if it allowed the forfeiture of a third party's interest, the forfeiture would become an in rem action and the third party could contest the forfeiture on more than ownership grounds); *United States v. O'Dell*, 247 F.3d 655, 680 (6th Cir. 2001) (recognizing that criminal forfeiture "entitles the government to forfeiture of a convicted defendant's interests and nothing more") (citation omitted); *United States v. Gilbert*, 244 F.3d 888, 919 (11th Cir. 2001) ("Because it seeks to penalize the defendant for his illegal activities, in personam forfeiture reaches only that property, or portion thereof, owned by the defendant.") (citation omitted), *superseded on other grounds as recognized in United States v. Marion*, 562 F.3d 1330, 1341 (11th Cir. 2009). The relation back doctrine, however, codified at 21 U.S.C. §§ 853(c) and 853(n)(6), provides that the government's interest in forfeitable property vests at the time of the offense giving rise to the forfeiture, and that property transferred to a third party after that time may be forfeited.

Even though criminal forfeiture is executed after conviction, the government should plan for criminal forfeiture during the investigation and at indictment. Pre-indictment seizure warrants can be used to seize infringing items (whether or not they are the property of a target). Moreover, the indictment should include separate forfeiture charges that identify any property that is forfeitable pursuant to the charged offenses. For forfeiture language to include in an indictment, prosecutors should consult the forfeiture expert in their office or the Criminal Division's Asset Forfeiture and Money Laundering Section at (202) 514-1263.

Criminal forfeiture is available for all IP offenses except violations of the DMCA. *See* 18 U.S.C. § 2323(b).

a. Proceeds

Generally, the government can obtain criminal forfeiture of proceeds from IP offenses whenever those proceeds are civilly forfeitable. *See* 18 U.S.C. § 2323(b)(1); 28 U.S.C. § 2461(c).

Independently, where a defendant has engaged in a monetary transaction involving the proceeds of an intellectual property offense, "knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity"—regardless of whether the crime is listed in 18 U.S.C. § 1956(c)(7)—the defendant may also be charged, and the proceeds

subject to forfeiture, under the money laundering statute directly. *See United States. v. Turner*, 400 F.3d 491 (7th Cir. 2005) (holding that the defendant need not know the actual source of the money, but only that it came from "some illegal activity"); *see also United States v. Khalil*, No. CR. A. 95-577-01, 1999 WL 455698 (E.D. Pa. June 30, 1999) (forfeiture involving counterfeiting popular music).

b. Infringing Items, Other Contraband, and Facilitating Property

Similarly, criminal forfeiture of contraband from, and facilitating property for, IP offenses is available whenever those materials are civilly forfeitable. *See* 18 U.S.C. § 2323(b)(1).

6. Domain Name Forfeiture

Increasingly, IP crimes are being perpetrated by website operators who are either unknown or outside the criminal jurisdiction of the United States. Their domain names, however, which point visitors to the sites, are often controlled by registrars and registries inside the United States. While it may be impractical or impossible to prosecute the operators themselves, forfeiture of the domain names may well be appropriate if they are facilitating the sale of infringing or counterfeit goods.

Domain name forfeiture can be a high-visibility action with an important deterrent effect. It is most suitable, however, when a website is being used solely or largely for illegal activities. One must consult with the Criminal Division's Asset Forfeiture and Money Laundering Section at (202) 514-1263 if the domain name is used for a combination of legal and illegal activities, such as constitutionally protected speech mixed with illegal transactions, or the domain name is used to run an ongoing business that is not engaging in predominately illegal activity.

The forfeiture statutes define "property" to include intangible property, such as licenses and rights. *See* 18 U.S.C. § 981(a)(1)(E); 21 U.S.C. § 853(b)(2); *United States v. Dicter*, 198 F.3d 1284 (11th Cir. 1999) (medical license). Registrants have intangible rights in their domain names. *Kremen v. Cohen*, 337 F.3d 1024, 1029 (9th Cir. 2003). Those rights could be characterized as either property rights or contract rights. *See, e.g., Dorer v. Arel*, 60 F. Supp. 2d 558, 561 (E.D. Va. 1999).

To forfeit a domain name, it is necessary to prove a nexus between the domain and the criminal offense. *See* 18 U.S.C. § 981(a); 21 U.S.C. § 853(a).

Often, the easiest way to establish this nexus is to argue that the domain facilitates the offense.

In civil forfeiture, to prove that a domain name facilitates the offense, it is necessary to show a "substantial connection" between the domain name and the offense. 18 U.S.C. § 981(c)(3) (civil forfeiture). A substantial connection or nexus can be shown by demonstrating that the domain name points to a computer that, in turn, is used in the offense. For example:

- the domain name points to a web server which hosts an online pharmacy selling counterfeit drugs; or
- the domain name points to a file server or cyber locker that offers pirated movies, music, or software for download.

a. The Steps in Domain Name Forfeiture

Below is a brief summary of the domain name forfeiture process. For more specific direction, and to obtain copies of sample documents, please contact CCIPS at (202) 514-1026 or the Criminal Division's Asset Forfeiture and Money Laundering Section at (202) 514-1263.

i. Seize (and Restrain) the Domain Name

A domain name is restrained by ordering the registrar not to permit the registrant to move the domain name to another registrar. This prevents the registrant from moving the domain name to a registrar outside the United States. A domain name is seized by placing it in a state where it no longer points to any server. Any email sent to the domain will bounce; any web browers trying to download a page from the domain will get a "host not found" error.

For IP crimes, the simplest approach is to seize and restrain the domain name civilly, using a seizure warrant issued under 18 U.S.C. § 981(b), which is made applicable by 18 U.S.C. § 2323(a)(2) to all IP crimes except DMCA violations. The investigative agency applies ex parte for a warrant. The warrant is granted if "there is probable cause to believe that the property is subject to forfeiture." 18 U.S.C. § 981(b)(2)(B).

There are two criminal forfeiture methods of seizure for domain names, both of which are made applicable by 18 U.S.C. § 2323(b)(2)(A) to all IP crimes except DMCA violations. The first method is to obtain a protective order under 21 U.S.C. § 853(e)(1). This is simplest to do right after an indictment, but it can also be done before an indictment. These orders have

nationwide scope. 21 U.S.C. § 853(l). Protective orders, however, do not allow one to "seize" the domain name by turning it off.

The second and preferred method, which does permit turning off the domain name, is to obtain a "warrant of seizure" issued under 21 U.S.C. § 853(f). The standard of proof is "probable cause to believe that the property to be seized would, in the event of a conviction, be subject to forfeiture," and that a protective order will not be sufficient. *Id.* These warrants have nationwide scope. 21 U.S.C. § 853(l). To establish that a protective order is not sufficient, one must establish the need to turn off the domain name now. For most sites peddling infringing or counterfeit goods, this should be fairly straightforward—unless the domain name is turned off, customers will continue to purchase unsafe or substandard goods, and rights holders will continue to suffer lost sales.

ii. Forfeit the Domain Name

When a domain name is forfeited, it becomes property of the United States. The former registrant loses all rights to, and control over, the domain name.

If this is a criminal seizure (i.e., the defendant owns the domain name), the indictment or information must identify the domain name as property to be forfeited. Fed. R. Crim. P. 32.2(a). One should include the domain names in the description of property to be forfeited, for example: "any personal property … including, but not limited to, the following Internet domain names: illegaldrugs.com." One should identify only the second-level domain names and should not include the prefixes "www" or "http" or refer to the domain names as "websites."

iii. Forfeiture as Part of a Plea Agreement

Domain name forfeiture can and ought to be included in a plea agreement, especially if the defendant was using the associated website to market counterfeit and/or infringing goods. If there is a parallel civil forfeiture proceeding, the defendant can agree not to contest forfeiture there. Otherwise, the defendant should consent in writing—the paperwork is ordinarily available from the registrar—to the voluntary transfer of the domain name to the United States.

iv. The Government's Use of the Domain Name

Once the United States successfully seizes a domain name, it retains possession until the registration period expires. Many domain names are

registered only for a year or two at a time. Once that period expires, the seizing agency would have to renew the registration or the name would go back on the open market.

The seizing agency may choose to post its own message or banner at the domain informing visitors that the name was seized because it was facilitating the sale of counterfeit or infringing goods in violation of federal law. The agency can then monitor the number of visitors who view the banner in order to measure its effect.

7. Interbank Account Seizures of Foreign Bank Funds

In 2001, Congress enacted 18 U.S.C. § 981(k) as part of the USA Patriot Act. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, § 319, 115 Stat. 272, 311-12 (2001). This civil forfeiture provision allows the United States to recover criminal proceeds that have been deposited in a foreign bank account by filing a civil forfeiture action—not against the funds in the foreign account itself, but against the funds that the foreign bank has on deposit in the United States at a domestic financial institution. It is not necessary for the Government to establish that the seized funds are directly traceable to the funds that were deposited into the foreign financial institution. Only the person who owned the forfeitable funds at the time they were deposited into the foreign bank has standing to contest the forfeiture. The foreign bank does not have standing to object to the forfeiture action.

Though the provision was aimed originally at terrorism, it can be useful in IP investigations. Used judiciously, it facilitates the seizure of proceeds from the sale of counterfeit and infringing goods by website operators who are outside United States criminal jurisdiction, and/or in countries with no extradition treaty with the U.S.—yet depend primarily on U.S. customers whose payments must pass through a domestic financial institution before moving into foreign accounts.

The Criminal Division's Asset Forfeiture and Money Laundering Section must approve the seizure of funds under § 981(k).

IX.

Charging Decisions

A. Introduction

In determining whether to charge an intellectual property crime, federal prosecutors should generally consider the same factors that are weighed with respect to any other federal offense. The principal resource is Chapter 9-27.000 of the *United States Attorneys' Manual* (USAM) ("Principles of Federal Prosecution"). Ordinarily, the prosecutor "should commence or recommend Federal prosecution if he/she believes that the person's conduct constitutes a Federal offense and that the admissible evidence will probably be sufficient to obtain and sustain a conviction." USAM 9-27.220.

This directive is not absolute. Even a provable case may be declined in three situations: when prosecution would serve no substantial federal interest; when the person is subject to effective prosecution in another jurisdiction; or when there exists an adequate non-criminal alternative to prosecution. *Id.* Broken down further, the relevant considerations include:

- The federal interest in intellectual property crimes.
- Federal law enforcement priorities.
- The nature and seriousness of the offense.
- The deterrent effect of prosecution.
- The individual's culpability in connection with the offense.
- The individual's criminal history.
- The individual's willingness to cooperate in the investigation or prosecution of others.
- The probable sentence and other consequences of conviction.
- Whether the person is subject to prosecution in another jurisdiction.
- The adequacy of alternative non-criminal remedies.
- Special considerations for deciding whether to charge corporations.

This chapter briefly discusses how some of these factors apply specifically to intellectual property crimes.

As discussed in Chapter IV, there are additional requirements and factors that apply in the prosecution of economic espionage cases under 18 U.S.C.

§ 1831. The Assistant Attorney General for the National Security Division must approve the filing of any charges under § 1831. USAM 9-2.400, 9-59.100. Additionally, USAM 9-59.110 provides that "[p]rosecutors are strongly urged to consult with the Computer Crime and Intellectual Property Section before initiating prosecutions under 18 U.S.C. § 1832." In economic espionage and trade secret cases, USAM 9-59.100 highlights the following factors in determining whether to commence prosecution:

a) the scope of the criminal activity, including evidence of involvement by a foreign government, foreign agent or foreign instrumentality;
b) the degree of economic injury to the trade secret owner;
c) the type of trade secret misappropriated;
d) the effectiveness of available civil remedies; and
e) the potential deterrent value of the prosecution.

B. The Federal Interest in Intellectual Property Crimes

In determining whether a particular prosecution would serve a substantial federal interest, the prosecutor should weigh all relevant factors. USAM 9-27.230. Several factors that have specific application to intellectual property crimes are discussed below.

1. Federal Law Enforcement Priorities

"[F]rom time to time the Department establishes national investigative and prosecutorial priorities. These priorities are designed to focus Federal law enforcement efforts on those matters within the Federal jurisdiction that are most deserving of Federal attention and are most likely to be handled effectively at the Federal level." USAM 9-27.230(B)(1) (comment).

Because of the importance of intellectual property to the national economy and the scale of intellectual property theft, intellectual property crime continues to be a law enforcement priority. Intellectual property theft worldwide costs American companies billions per year. The Justice Department has therefore made the enforcement of intellectual property laws a high priority. Through its Intellectual Property Task Force, the Department has identified four categories of IP investigations and prosecutions that deserve special attention: offenses that involve (1) health and safety; (2) links to organized criminal networks; (3) large scale commercial counterfeiting and piracy, particularly occurring online;

and (4) trade secret theft or economic espionage. *See* U.S. Dep't of Justice, *PRO IP Act Annual Report FY2011,* at 16 (2011).

To meet these and other priorities, the Department has trained a national network of specialized prosecutors designated "Computer Hacking and Intellectual Property" (CHIP) coordinators, at least one of whom is located in each of the nation's ninety-four United States Attorneys' Offices, with greater numbers in the twenty-five CHIP units located in districts that experience some of the highest concentrations of computer and intellectual property crimes. Under this program, there are more than 260 CHIP prosecutors around the country. At the national and international level, intellectual property prosecutions are coordinated by the Department's Computer Crime and Intellectual Property Section (CCIPS) in Washington, D.C.

Notably, and in part to support these efforts, the Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008 increased both the penalties for intellectual property offenses and the resources available to law enforcement for the investigation and prosecution of IP crimes. Among other things, the PRO-IP Act: (i) increased the maximum penalties for trademark counterfeiting violations resulting in serious bodily injury or death; (ii) made restitution and criminal forfeiture mandatory for virtually all intellectual property offenses; (iii) established a federal grant program to provide state and local law enforcement agencies with funds for intellectual property crime training, prevention, enforcement and prosecution; (iv) authorized and later appropriated funding for the assignment of 51 Federal Bureau of Investigation ("FBI") special agents specifically to investigate intellectual property crimes as well as 15 additional CHIP positions; and (v) required the submission of annual reports to Congress from both the Attorney General and the Director of the FBI on their progress in implementing the objectives of the PRO-IP Act. Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act, Pub. L. No. 110-403, §§ 205, 206, 401, 402, 404, 122 Stat. 4256, 4261-64, 4271-72, 4274-4277 (2008).

CCIPS can help evaluate whether a particular intellectual property crime poses a matter of federal priority. CCIPS can be reached at (202) 514-1026.

2. The Nature and Seriousness of the Offense

As with other offenses, intellectual property crimes vary in their nature and seriousness. It is therefore essential to consider each case on its own facts.

The offense's nature and seriousness are indicated by the usual factors, with special importance placed on threats to health or safety, *see* U.S.S.G. § 2B5.3(b)(5); the volume of infringement as measured by the amount of revenue and profit, *see* § 2B5.3(b)(1), cmt. n.2; the involvement of organized crime, *see* § 2B5.3 cmt. n.4(B); and whether substantial harm was done to the reputation of the rights holder, *see id.* cmt. n.4(A).

Other considerations that are more particular to intellectual property offenses include the following:

- **Federal criminal prosecution is most appropriate in the most egregious cases.** The criminal intellectual property statutes punish only a subset of the conduct that is punishable under civil intellectual property laws. Even then, the government must prove its case beyond a reasonable doubt, including a high state of mens rea.
- **Limited federal resources should not be diverted to prosecute an inconsequential case or a case in which the violation is only technical.** Even some branches of civil intellectual property law recognize the maxim, "de minimis non curat lex."
- **Federal prosecution is most appropriate when the questions of intellectual property law are most settled.** However, federal prosecutors should not hesitate to apply settled intellectual property concepts in innovative ways to new schemes and new technology.
- **Victims have a broad range of civil remedies that include restitution, damages, punitive or quasi-punitive damages, injunctions, court costs, and attorneys' fees.** See Section D. of this Chapter.
- **The more strongly an intellectual property owner acts to protect its rights, the stronger the interest in prosecution.** *Id.*
- **Many intellectual property offenses include multiple victims: not only the owners of the intellectual property that was infringed, but also customers who were defrauded.** Both classes of victim deserve protection, and one class's lack of interest in prosecution should not countermand prosecution when the other class's interest is strong.
- **The sources or manufacturers of infringing goods and services are generally more worthy of prosecution than distributors.** *Cf.* U.S.S.G. § 2B5.3(b)(3) (adjusting offense level for infringement offenses involving the manufacturing, uploading or smuggling of infringing items by 2 levels, with a minimum offense level of 12).

- **Counterfeit goods or services that endanger the public's health or safety deserve the highest consideration for prosecution.** *See* U.S. Dep't of Justice, *PRO IP Act Annual Report FY2011*, at 16 (2011); *cf.* U.S.S.G. § 2B5.3(b)(5) (adjusting offense level for infringement offenses involving "conscious or reckless risk of death or serious bodily injury [or] possession of a dangerous weapon" by 2 levels, with a minimum offense level of 14).

3. The Deterrent Effect of Prosecution

Some infringers are undeterred by civil liability. They treat civil remedies as a cost of doing business and continue their infringement after civil sanctions, albeit with different products or under a different corporate guise. Criminal prosecution can better deter a persistent violator from repeating his or her crime.

Criminal prosecution may also further general deterrence. Individuals may commit intellectual property crimes not only because some are relatively easy to commit, such as copying music, but also because they do not fear prosecution. But one person's relatively small-scale violations, if permitted to take place openly and notoriously, can lead others to believe that such conduct is tolerated. While some counterfeiting or piracy offenses may not result in provable direct loss to a victim, the widespread commission of such crimes can devastate the value of intellectual property rights in general.

Criminal prosecution plays an important role in establishing the public's understanding of what conduct is acceptable and what is not. Vigorous prosecution changes the public's calculus. Put simply, more individuals will be deterred from committing intellectual property offenses if they believe they will be investigated and prosecuted.

4. The Individual's History of Criminal Offenses and Civil Intellectual Property Violations

Repeat criminal offenders are especially worthy of prosecution. *See* USAM 9-27.230(B)(5) (comment). The repeat-offender provisions in the intellectual property crime statutes, *e.g.,* 18 U.S.C. § 2320(b)(1)(B), and the United States Sentencing Guidelines ensure that repeat offenders receive stiffer sentences.

In addition to the defendant's criminal history, it is also appropriate to consider his or her history of civil intellectual property violations. When infringers consider civil penalties merely a cost of doing business, criminal

enforcement is particularly appropriate. Sources for determining the defendant's history of civil intellectual property offenses include civil litigation records (which are often searchable online), the victim's legal department and private investigators, and any state consumer protection agencies to which consumers might have complained. Another relevant consideration concerns any infringement or misappropriation conduct following the issuance of cease and desist letters or injunctive orders.

5. The Individual's Willingness to Cooperate in the Investigation or Prosecution of Others

As discussed in Section B.2. of this Chapter, the sources of counterfeit or pirated goods or services are especially worthy of prosecution. Special consideration should be given to targets who are willing to cooperate in an investigation that leads to a source's prosecution.

This includes the prosecution of foreign sources. In recent years, the Department of Justice has worked extensively with foreign law enforcement agencies to investigate and prosecute foreign violators, both by extraditing foreign violators to the United States and by coordinating searches and prosecutions simultaneously in the United States and abroad. CCIPS has regular contact with foreign prosecutors and law enforcement agencies with an interest in intellectual property crime. Therefore, for assistance in investigating or prosecuting offenses with an international dimension, contact CCIPS at (202) 514-1026.

C. Whether the Person Is Subject to Prosecution in Another Jurisdiction

One situation in which a prosecutor may decline prosecution despite having a provable case occurs when the putative defendant is subject to effective prosecution in another jurisdiction. USAM 9-27.240. Relevant to this inquiry is the strength of the other jurisdiction's interest in prosecution; the other jurisdiction's ability and willingness to prosecute effectively; the probable sentence or other consequences of conviction in the other jurisdiction; and any other pertinent factors. *Id.*

The primary question will often not be whether the case could be prosecuted by another U.S. Attorney's Office, but rather whether it could be prosecuted by state, local, or foreign authorities. USAM 9-27.240(B) (comment). State, local,

or foreign law enforcement may or may not be a viable alternative to federal prosecution. Federal intellectual property laws generally do not preempt state and local intellectual property laws. For example, in trade secret and economic espionage cases, Congress expressly anticipated that other appropriate remedies may be considered. The Economic Espionage Act explicitly provides that the statute does not "preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret." 18 U.S.C. § 1838.

The only relevant area of intellectual property in which there is broad federal preemption is copyright infringement, but even in that area states have passed some creative laws that indirectly criminalize conduct involving some pirated works. *Compare* 17 U.S.C. § 301 (copyright preemption); *R.W. Beck, Inc. v. E3 Consulting, LLC*, 577 F.3d 1133, 1148-49 (10th Cir. 2009) (holding Copyright Act preempted state common law claims for unfair competition and unjust enrichment); *Kodadek v. MTV Networks, Inc.*, 152 F.3d 1209, 1212-13 (9th Cir. 1998) (holding state law unfair competition claim preempted where complaint expressly based the claim on rights granted by the Copyright Act); *Kregos v. Associated Press*, 3 F.3d 656, 666 (2d Cir. 1993) (holding state law unfair competition and misappropriation claims preempted when based solely on the copying of protected expression in forms); *Wnet v. Aereo*, No. 12 Civ. 1543(AJN), 2012 WL 1850911, at *11 (S.D.N.Y. May 18, 2012) (holding state law unfair competition claim preempted by Copyright Act); *People v. Williams*, 920 N.E.2d 446, 458 (Ill. 2009) (holding Illinois antipiracy provision preempted by Copyright Act); *and State v. Perry,* 697 N.E.2d 624 (Ohio 1998) (holding that federal copyright law preempted prosecution in case involving defendant's use of computer software on his bulletin board); *with Anderson v. Nidorf*, 26 F.3d 100, 102 (9th Cir. 1994) (holding California anti-piracy statute not preempted by federal copyright law in illegal sound recording case); *Briggs v. State*, 638 S.E.2d 292, 295 (Ga. 2006) (holding Georgia statute criminalizing the sale of recordings without a label identifying the "transferor" not preempted by federal copyright law); *State v. Awawdeh*, 864 P.2d 965, 968 (Wash. Ct. App. 1994) (holding Washington statute not preempted by federal copyright law in illegal sound recording case); *and People v. Borriello*, 588 N.Y.S.2d 991, 996 (N.Y. App. Div. 1992) (holding New York statute not preempted by Copyright Revision Act in illegal video recording case).

D. The Adequacy of Alternative Non-Criminal Remedies

Department of Justice policy allows a prosecutor to decline criminal prosecution in a situation that could be adequately addressed by non-criminal remedies. USAM 9-27.220(A)(3). Almost every federal intellectual property crime has an analogue in civil law—be it state or federal—and those laws generally offer victims generous relief, such as injunctions, restitution, damages, punitive and quasi-punitive damages, court costs, attorneys' fees, and even ex parte seizure of a defendant's infringing products. *See* 15 U.S.C. §§ 1114, 1116-1117 (trademark); 17 U.S.C. §§ 501-505 (copyright). Imported and exported infringing merchandise can also be subject to administrative forfeiture and fines imposed by United States Customs and Border Protection. *See, e.g.*, 17 U.S.C. §§ 602, 603(c) (copyright), 19 U.S.C. § 1526(e)-(f) (trademark). The availability and adequacy of these remedies should be carefully considered when evaluating an intellectual property case.

The prosecutor should also consider whether existing civil remedies have been or are likely to deter a particular defendant. For those undeterred by civil suits and remedies, criminal prosecution may be more appropriate. When the defendant has violated an earlier civil order, however, civil or criminal penalties for contempt of court may be an acceptable alternative to prosecution for criminal intellectual property violations.

Finally, when the violator's conduct is persistent, unsafe, profit-oriented, fraudulent, or physically invasive, civil remedies may not fully capture the wrongfulness of the defendant's conduct. In such cases, criminal prosecution may be preferred.

Although the government may prosecute even if the victim has not exhausted its civil and administrative remedies, the government should consider the victim's pursuit of alternative remedies. The putative defendant's conduct in response should also be examined.

E. Special Considerations in Deciding Whether to Charge Corporations and Other Business Organizations

Corporations and other business organizations are often used to commit intellectual property crimes. The decision whether to charge a business organization involves numerous considerations. Department of Justice policy on such charging decisions is generally set forth in the Principles of Federal Prosecution of Business Organizations. USAM 9-28.000. This guidance applies to intellectual property crimes in the same manner as to other crimes. In deciding whether prosecution of a business organization is appropriate, relevant factors include:

- The nature and seriousness of the offense, including the risk of harm to the public, and applicable policies and priorities, if any, governing the prosecution of corporations for particular categories of crime (*see* USAM 9-28.400);
- The pervasiveness of wrongdoing within the corporation, including the complicity in, or the condoning of, the wrongdoing by corporate management (*see* USAM 9-28.500);
- The corporation's history of similar misconduct, including prior criminal, civil, and regulatory enforcement actions against it (*see* USAM 9-28.600);
- The corporation's timely and voluntary disclosure of wrongdoing and its willingness to cooperate in the investigation of its agents (*see* USAM 9-28.700);
- The existence and effectiveness of the corporation's pre-existing compliance program (*see* USAM 9-28.800);
- The corporation's remedial actions, including any efforts to implement an effective corporate compliance program or to improve an existing one, to replace responsible management, to discipline or terminate wrongdoers, to pay restitution, and to cooperate with the relevant government agencies (*see* USAM 9-28.900);
- Collateral consequences, including whether there is disproportionate harm to shareholders, pension holders, employees, and others not proven personally culpable, as well as impact on the public arising from the prosecution (*see* USAM 9-28.1000);

- The adequacy of the prosecution of individuals responsible for the corporation's malfeasance (*see* USAM 9-28.300); and
- The adequacy of remedies such as civil or regulatory enforcement actions (*see* USAM 9-28.1100).

X.
Victims of Intellectual Property Crimes—Ethics and Obligations

> But justice, though due to the accused, is due to the accuser also.... We are to keep the balance true.

Justice Benjamin Cardozo, *Snyder v. Massachusetts*, 291 U.S. 97, 122 (1934).

Many victims of intellectual property ("IP") offenses are atypical, in that they often have substantial resources to protect their rights by investigating, pursuing, and deterring infringers independent of law enforcement. For instance, businesses often pool their resources in industry groups that undertake enforcement actions on their behalf. See Appendix G (listing trademark and copyright organization contacts). These groups sometimes investigate violations independently and refer the results to law enforcement with a request to bring charges. They may even seek to contribute resources to law enforcement agencies or multi-agency task forces organized to focus on IP offenses. Whether an IP victim can enforce its rights through civil or administrative processes may influence whether criminal prosecution is warranted (see Chapter IX of this Manual), and if so, what charges and strategy are appropriate. The fact that IP rights holders sometimes can address IP crime on their own does not, however, diminish their rights under federal law.

Although rights holders are often the primary victims in IP offenses, consumers are victimized also. Consumers may be defrauded into buying counterfeits that are second-rate or, worse, unsafe, while consumers who purchase authentic goods end up paying higher prices to offset industry losses caused by counterfeiting and piracy.

A. Victims' Rights

Beginning with the passage of the Victim and Witness Protection Act of 1982, Pub. L. No. 97-291, 96 Stat. 1248 (1982), Congress has enacted numerous statutes that protect victims' rights during the investigation, prosecution, and

sentencing stages of criminal proceedings. Most recently, Congress revised and recodified victims' rights laws in the Justice for All Act of 2004, Pub. L. No. 108-405, 118 Stat. 2260 (2004). The Department issued revised guidance for implementing the Justice for All Act in the *Attorney General Guidelines for Victim and Witness Assistance* (2012 ed.) ("*AG Guidelines*"), *available at* http://www.justice.gov/olp/pdf/ag_guidelines2012.pdf.

Generally, the Justice for All Act requires Department of Justice employees to make their best efforts to notify victims of the following rights:

1. The right to be reasonably protected from the accused
2. The right to reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime or any release or escape of the accused
3. The right not to be excluded from any such public court proceeding, unless the court, after receiving clear and convincing evidence, determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding
4. The right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding
5. The reasonable right to confer with the attorney for the government in the case
6. The right to full and timely restitution as provided in law
7. The right to legal proceedings free from unreasonable delay
8. The right to be treated with fairness and with respect for the victim's dignity and privacy

See 18 U.S.C. § 3771(a), (c)(1); *AG Guidelines*, arts. V.C-V.J. Apart from these enumerated rights, the prosecutor has an independent obligation under the Act to advise the victim of his or her right to counsel in connection with the rights established by the Act. *See* 18 U.S.C. § 3771(c)(2); *AG Guidelines*, art. V.B.2.

The Act also creates several enforcement mechanisms. If the government or a victim believes the victim's rights are being violated, relief is possible by way of motion in the trial court and ultimately a petition for writ of mandamus in the Court of Appeals. *See* 18 U.S.C. § 3771(d)(3); *AG Guidelines*, art. V.K. If the victim's rights are violated, the Act does not permit a motion for a new trial, but does provide for re-opening a plea or sentence. 18 U.S.C. § 3771(d)

(5). Finally, although the Act does not authorize suits against government personnel, it requires the Department to create an administrative authority within the Department to receive and investigate complaints, and impose disciplinary sanctions for willful or wanton non-compliance. *See* 18 U.S.C. § 3771(f)(2); *AG Guidelines*, art. V.B.4; 28 C.F.R. § 45.10 (2005).

For purposes of enforcing these rights, the Justice for All Act defines a victim as "a person *directly and proximately harmed* as a result of the commission of a Federal offense or an offense in the District of Columbia." *See* 18 U.S.C. § 3771(e) (emphasis added); *see also AG Guidelines*, art. III.C.1. A victim may be an individual, a corporation, company, association, firm, partnership, society, or joint stock company. *See* 1 U.S.C. § 1 (defining "person"); *AG Guidelines*, art. III.C.2. In considering whom to classify as a victim, prosecutors may consider whether those who were injured during the commission of a federal crime were indeed "directly and proximately harmed" by the offense within the meaning of 18 U.S.C. § 3771(e), particularly in cases where there are hundreds or even thousands of potential victims.

The Act also contains a section on "Multiple Crime Victims" to address notification in cases involving large numbers of victims. This provision, which is of particular interest in cases involving the large-scale distribution of pirated or counterfeit goods, states:

> In a case where the court finds that the number of crime victims makes it impracticable to accord all of the crime victims the rights described in subsection (a), the court shall fashion a reasonable procedure to give effect to this chapter that does not unduly complicate or prolong the proceedings.

18 U.S.C. § 3771(d)(2); *see also AG Guidelines*, arts. III.K, V.D.2, V.E.4. For instance, in an online piracy prosecution with hundreds or thousands of victims from different content industries, it is often impractical for a prosecutor to notify every rights holder. In such cases, the prosecutor should consider, at a minimum, notifying and enlisting the assistance of any trade organizations that represent multiple victim rights holders. The prosecutor could then seek court approval for an alternative procedure authorizing him or her to notify such representatives in lieu of notifying all rights holders.

The Act states that "[n]othing in this chapter shall be construed to impair the prosecutorial discretion of the Attorney General or any officer under his direction." 18 U.S.C. § 3771(d)(6). Congress clearly did not intend the Act

to be implemented in a way that hinders prosecutorial discretion in addressing issues of victims' rights and notification.

The Act did not alter other provisions that protect victimized rights holders. In all criminal prosecutions, a pre-sentence report must contain verified information containing an assessment of the impact on any individual against whom the offense has been committed. Fed. R. Crim. P. 32(d)(2)(B). Additionally, most intellectual property statutes guarantee victims (including producers and sellers of legitimate works, rights holders, and their legal representatives) the right to submit a victim impact statement identifying the extent and scope of their injury and loss prior to sentencing. *See* 18 U.S.C. §§ 2319(e), 2319A(d), 2319B(e), 2320(e).

B. The Victim's Role in the Criminal Prosecution

The fact that victims of IP crime have access to civil remedies raises several issues during criminal prosecution.

1. Reporting an Intellectual Property Crime

It is recommended that victims of intellectual property crimes document all investigative steps, preserve evidence, and contact law enforcement as soon as possible. Victims can report intellectual property crimes to appropriate law enforcement agencies as described in the referral guidelines contained in Appendix H of this Manual.

2. Ethical Concerns When the Criminal Prosecution Results in an Advantage in a Civil Matter

Like other crime victims, IP rights holders are often interested in securing economic and other relief, but, unlike other types of crime victims, rights holders have strong civil enforcement tools and resources that they often use to aggressively pursue civil remedies. Prosecutors are obligated by statute and policy to assist victims in obtaining restitution and other remedies, but prosecutors are also obligated to serve the public interest. Occasionally, those interests may be in tension. In this regard, prosecutors should consider whether or to what extent IP victims are using the threat of criminal prosecution to advance their private interests and to what extent the government can offer a defendant concessions in prosecution or sentencing in exchange for the defendant's agreement to compensate the victim or mitigate the harm the defendant has caused.

a. Victims Who Seek Advantage by Threats of Criminal Prosecution

It is commonplace for an IP-owner's attorney to send a merchant a letter directing him to cease and desist sales of infringing merchandise. If the merchant continues to infringe, the letter will be solid evidence of the defendant's mens rea during any ensuing criminal case.

Sometimes the IP-owner's letter will include an express or implied threat to seek criminal prosecution should the merchant persist. The extent to which it is ethically permissible for a lawyer to threaten to press criminal charges as a means to advance a civil cause of action is unclear. The lack of clarity stems in part from a patchwork of inconsistent ethical rules. The ABA's Model Code of Professional Responsibility (adopted in 1969, amended in 1980) explicitly prohibited strategic threats of prosecution: "A lawyer shall not present, participate in presenting, or threaten to present criminal charges solely to obtain an advantage in a civil matter." Model Code of Prof'l Responsibility DR 7-105A (1980). The ABA's Model Rules of Professional Conduct, adopted in 1983, omitted the rule as "redundant or overbroad or both." *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Ethics Op. 92-363 (1992) (allowing a lawyer to use a threat of a criminal referral to obtain advantage if the civil claim and criminal matter are related and well-founded). Not all states have dropped the old rule, and some have adopted other specific provisions addressing the issue. *Compare Office of Disciplinary Counsel v. King*, 617 N.E.2d 676, 677 (Ohio 1993) (disciplining a lawyer under the old rule for threatening to seek prosecution unless opponent in property dispute paid disputed rent or vacated the property), *with* Or. Rules of Prof'l Conduct r. 3.4(g) (Or. State Bar 2005) (prohibiting such threats "unless the lawyer reasonably believes the charge to be true and if the purpose of the lawyer is to compel or induce the person threatened to take reasonable action to make good the wrong which is the subject of the charge").

Whatever the implication for the victim's lawyer, there is nothing unethical about the government's decision to prosecute the offender after such a threat has been made. The victim's threat does not present a legal or ethical obstacle for the prosecution. Instead, the concern for the government prosecutor is a strategic one, to the extent that the threat reflects on the victim's credibility or willingness to manipulate the criminal justice system for private gain. The victim's conduct in this regard is one factor among many to be considered in deciding whether to prosecute.

b. Global Settlement Negotiations

Ethical questions arise when the prosecution, victim, and defendant attempt to resolve all pending civil and criminal disputes in a global settlement agreement. While the answers to these questions are not entirely clear, there are some best practices that follow the guidelines cited above, Department policy, and strategic concerns.

First, it is often the better practice for the prosecutor to defer to the other parties to suggest a global disposition rather than be the first to suggest it. By adopting this approach, the prosecutor is less likely to create the appearance of overreaching:

> [T]he government can neither be, nor seem to be, trading money for relief or insulation from criminal prosecution or sentencing consequences. Such a trade-off not only would undermine the integrity of the prosecutorial process, but also raises formidable fairness concerns, with wealthy defendants better able to reach global settlements than poor ones.
>
> * * *
>
> Many prudent Assistant United States Attorneys consider global settlements to have an appropriate and ethical role in resolving parallel proceedings, but follow a rule of not introducing or suggesting such a disposition. If opposing counsel raise[s] the issue, it may be responded to and pursued by government attorneys in close consultation with supervisors, and mindful of the ethics issues.

Office of Legal Education, U.S. Dep't of Justice, *Federal Grand Jury Practice* § 12.12 (2008) (concerning parallel proceedings and global settlements).

Second, it is the better practice to limit the negotiations to matters of criminal law. For example, as discussed in Section B.3.a. of this Chapter, although some civil remedies will award a victim of IP theft with treble damages, treble damages cannot be awarded under the criminal restitution statutes. *See* 18 U.S.C. § 3663(b), 3663A(b), 3664(f)(1)(A). See also Chapter VIII, Section D.3. of this Manual for a discussion of how to determine restitution measures). However, the criminal statutes permit restitution to be ordered "to the extent agreed to by the parties," 18 U.S.C. § 3663(a)(3), and allow for the defendant to provide services in lieu of money, 18 U.S.C. §§ 3663(b)(5), 3664(f)(4)

(C). Therefore, it is perfectly appropriate for the government to require full restitution as a condition of a plea agreement. See Chapter VIII, Sections D.1.-.2. of this Manual.

Clearly, the government may not use the threat of unsupported charges to obtain advantage for a civil plaintiff. Model Rule of Professional Conduct 3.8 prohibits a prosecutor from seeking charges that the prosecutor knows are not supported by probable cause, and Rule 3.1 prohibits any advocate from asserting frivolous claims. Rule 4.1 requires a lawyer to be truthful. Even a well-founded threat of criminal prosecution may be unethical if intended merely to "embarrass, delay or burden a third person." Model Rules of Prof'l Conduct R. 4.4 (2003).

Finally, there are strategic concerns. A judge or jury might react negatively if the victim or prosecutor appears to be threatening more serious consequences in the criminal case as leverage in the civil disposition. Although the prosecutor must at all times keep the victim informed of the progress of the criminal case, including discussion of a plea offer (see Section A. of this Chapter), it is ultimately the prosecutor who must decide how, if at all, to attempt to resolve a criminal case, including all issues of restitution to the victim.

3. Parallel Civil Suits

> The civil and regulatory laws of the United States frequently overlap with the criminal laws, creating the possibility of parallel civil and criminal proceedings, either successive or simultaneous. In the absence of substantial prejudice to the rights of the parties involved, such parallel proceedings are unobjectionable under our jurisprudence.

Sec. & Exch. Comm'n v. Dresser Indus., Inc., 628 F.2d 1368, 1374 (D.C. Cir. 1980) (en banc) (footnote omitted). The topic of parallel civil suits is complex and largely beyond the scope of this Manual. For a more extensive discussion of parallel proceedings, see Office of Legal Education, U.S. Dep't of Justice, *Federal Grand Jury Practice* § 12 (2008). The following is a brief summary.

a. Private Civil Remedies

Victims of IP crimes have significant civil enforcement mechanisms and remedies against infringers. In civil actions, IP rights holders can recover damages, the defendant's profits, costs, attorney fees, and even statutory damages, which can be punitive or quasi-punitive. *See* 15 U.S.C.

§ 1117 (trademark infringement damages); 17 U.S.C. §§ 504 (copyright infringement), 505 (same), 1101 (bootlegged recordings of live musical performances), 1203 (DMCA); 18 U.S.C. § 2318(e) (illicit labels and counterfeit labels, documentation, and packaging for copyrighted works); *see also Getty Petroleum Corp. v. Island Transp. Corp.*, 862 F.2d 10, 13-14 (2d Cir. 1988) (holding punitive damages unavailable for federal trademark claims, but may be available for state infringement and unfair competition claims). Civil remedies also include injunctive relief against future infringement and seizure or impoundment of infringing goods. 15 U.S.C. §§ 1116, 1118 (trademark); 17 U.S.C. §§ 502 (copyright), 503 (same), 1101 (bootlegged recordings of live musical performances), 1203(b) (DMCA); 18 U.S.C. § 2318(e)(2)(A), (B) (illicit labels and counterfeit labels, documentation, and packaging for copyrighted works); *see also Chanel Inc. v. Gordashevsky*, 558 F. Supp. 2d. 532, 539-40 (D.N.J. 2008) (granting permanent injunction preventing defendant from engaging in future infringing conduct and transfer of infringing domain names to plaintiff).

Victims of trademark or copyright infringement can also seek the private counterpart of a search warrant: an ex parte seizure order, executed by law enforcement. 15 U.S.C. § 1116(d) (trademark); 17 U.S.C. § 503 (copyright); *see Columbia Pictures Indus., Inc. v. Jasso*, 927 F. Supp. 1075-77 (N.D. Ill. 1996) (sealed writ of seizure issued for pirated videos); *Time Warner Entm't Co. v. Does Nos. 1-2*, 876 F. Supp. 407, 410-15 (E.D.N.Y. 1994) (recognizing availability of seizure order for infringing goods, but denying the victims' ex parte request on Fourth Amendment grounds because it called for execution by private investigators and failed to describe the locations to be searched with particularity). A party seeking civil seizure of goods with counterfeit marks must first notify the United States Attorney to allow the government's intervention should the seizure affect the public interest in a criminal prosecution. 15 U.S.C. § 1116(d)(2).

Prosecutors should consider the availability and use of private civil remedies in deciding whether to prosecute an infringer criminally. See Chapter IX, Section D. of this Manual.

b. Advantages and Disadvantages of Parallel Civil and Criminal Proceedings

If the government prosecutes a defendant who is also a party to a pending civil case, the parallel proceedings raise their own set of issues:

Advantages

- The victim's private civil enforcement action brings additional statutory and equitable remedies to bear on a defendant.
- The victim's allocation of resources to the investigation may conserve government resources. Moreover, as discussed in Section C. of this Chapter, the victim's independent reasons for providing resources to advance the civil case may lessen the appearance of any potential conflict of interest.
- In the civil case, the plaintiff victim can compel discovery, which the prosecution can use and discuss with the victim without grand jury secrecy or operational concerns.
- A civil case presents the defendant with a difficult Fifth Amendment choice. If he submits to discovery, he may lock in his story, provide leads, disclose strategy, or furnish false exculpatory statements, all of which may assist the criminal prosecutor. If he asserts his privilege against self-incrimination in the civil matter, however, the jury in the civil case can be instructed that it may draw an adverse inference from his silence. *See, e.g., Baxter v. Palmigiano*, 425 U.S. 308, 318-19 (1976) (adverse inference from silence permissible in prison disciplinary proceedings); *Hinojosa v. Butler*, 547 F.3d 285, 291-95 (5th Cir. 2008); *ePlus Tech., Inc. v. Aboud*, 313 F.3d 166, 179 (4th Cir. 2002) (adverse inference permissible in civil RICO fraud case); *LaSalle Bank Lake View v. Seguban*, 54 F.3d 387, 390-91 (7th Cir. 1995) (same).
- A criminal conviction typically ends the civil case in the victim's favor, either because the victim can rely on the criminal court's restitution order, collateral estoppel conclusively establishes the defendant's wrongdoing in the civil case, or the conviction simply renders the defendant less willing to contest the civil case.

Disadvantages

- Given the availability of private, civil enforcement mechanisms, the court may view the criminal prosecution as a waste of judicial resources.
- The government loses control of a component of the investigation. Actions taken by private counsel and investigators for the civil case may not be in the criminal case's best interests.
- If the grand jury is used to gather evidence, secrecy concerns may require criminal investigators to withhold material information from the parties to the civil proceeding, although collecting evidence outside

the grand jury, such as through search warrants or administrative subpoenas, may allow the government to share information without breaching grand jury secrecy.

- The defendant can compel discovery in the civil case, which may generate inconsistent witness statements and provide insight into the prosecution's case. As a result, some prosecutors will seek to stay the civil case while the criminal case proceeds.

c. Stays and Protective Orders to Delay Civil Proceedings During Criminal Prosecution

If the disadvantages of parallel proceedings outweigh the advantages, the government may seek a protective order or a stay of the civil proceedings. There is ample authority for issuing a stay or protective order, especially when liberal civil discovery would allow a criminal target or defendant to interfere with the investigation or bypass restrictions on criminal discovery. *See, e.g., Degen v. United States*, 517 U.S. 820, 825-26 (1996) (holding that a stay may be sought in parallel civil forfeiture action); *United States v. Stewart*, 872 F.2d 957, 961-63 (10th Cir. 1989) (holding that a court handling a criminal case may have authority under Fed. R. Crim. P. 16(d) or 18 U.S.C. § 1514(a) to prevent parties in a parallel civil case from abusing witnesses or discovery procedures); *Sec. & Exch. Comm'n v. Dresser Indus.*, 628 F.2d 1368, 1376 n.20 (D.C. Cir. 1980) (en banc) (noting that the government may seek postponement of the noncriminal proceeding to prevent the criminal defendant from broadening his rights of criminal discovery against the government); *Campbell v. Eastland*, 307 F.2d 478, 490 (5th Cir. 1962) (holding that the public interest in criminal prosecution with limited discovery outweighed civil litigant's right to prepare case promptly); *see also* Office of Legal Education, U.S. Dep't of Justice, *Federal Grand Jury Practice* §§ 12.9,12.10 (2008).

When seeking a stay or protective order, the government should be prepared to address the following factors: (1) the extent to which issues in the criminal case overlap with those presented in the civil case; (2) the status of the criminal matter, especially whether the civil defendant has been indicted; (3) the interest of the plaintiff in proceeding expeditiously, as weighed against the prejudice caused by the delay; (4) the private interests of and burden on the defendant; (5) the interest of the court in case management and judicial resources; (6) the interest of non-parties; and (7) the public interest. *See, e.g., Louis Vuitton Malletier S.A. v. LY USA, Inc.*, 676 F.3d 83, 99-100 (2d Cir. 2012); *Microfinancial, Inc. v. Premier Holidays Int'l, Inc.*, 385 F.3d 72, 78 (1st

Cir. 2004); *Keating v. Office of Thrift Supervision*, 45 F.3d 322, 324-25 (9th Cir. 1995); *Eastwood v. United States*, No. 2:06-cv-164, 2008 U.S. Dist. LEXIS 106777, *9 (E.D. Tenn. Nov. 14, 2008); *Chao v. Fleming*, 498 F. Supp. 2d 1034, 1037 (W.D. Mich. 2007); *Benevolence Int'l Found. v. Ashcroft*, 200 F. Supp. 2d 935, 938 (N.D. Ill. 2002); *Trustees of the Plumbers and Pipefitters Nat'l Pension Fund v. Transworld Mech., Inc.*, 886 F. Supp. 1134, 1139 (S.D.N.Y. 1995).

C. Offers of Assistance From Victims and Related Parties

IP rights holders frequently offer to provide resources to assist the government with criminal investigations. Traditionally, law enforcement agencies have routinely accepted assistance from victims and citizens willing to do so in discharge of their civic duty. However, offers of assistance in investigations and litigation have increased in scope, variety, and monetary value. Consequently, at the prompting of the Department of Justice's Task Force on Intellectual Property, the Deputy Attorney General issued a May 2006 memorandum to all United States Attorneys and component heads on accepting resources from victims, related parties, and third parties for use in investigations and prosecutions. A copy of the memorandum, entitled Guidance for Acceptance of Assistance and Gifts from Private Parties for Use in Connection with Investigations and Litigation, may be found at http://www.justice.gov/dag/readingroom/dag-may262006.pdf.

Although this subsection tracks the Department's guidance closely and highlights certain issues, the reader is advised to refer to the memorandum itself before deciding on an appropriate response to an offer of resources. The reader should also refer to Appendix J of this Manual, which examines a variety of hypothetical offers of resources, such as private investigators offering information; victims offering meeting space, expert witnesses, purchase money to obtain counterfeit items, and storage space for seized items; and unrelated parties offering forensic tools and analysis, facilities from which to conduct an investigation, and expert witness services.

An offer of donated resources generally raises three issues. First is whether the donation of resources is permitted by laws, regulations, and Department directives limiting the acceptance of gifts. This will usually turn on whether the offered resources constitute a gift or the type of assistance traditionally provided by victims of crime, their related parties, and third parties. Second, is whether

the assistance is permitted by the rules of professional conduct regardless of whether the offered resources are considered to be gifts or assistance. And third, is whether the assistance will have an adverse impact on the prosecution, even if permissible under gift restrictions and rules of professional conduct. All three issues are addressed below.

1. Gift Issues

a. Applicable Law

The Attorney General has authority to "accept, hold, administer, and use gifts, devises, and bequests of any property or services for the purpose of aiding or facilitating the work of the Department of Justice." 28 U.S.C. § 524(d)(1). Gifts of money (including money derived from property) must be deposited in the Treasury for the benefit of the Department and may be distributed by order of the Attorney General. 28 U.S.C. § 524(d)(2).

In 1997, the Attorney General issued Department of Justice ("DOJ") Order 2400.2, *available at* http://www.justice.gov/jmd/ethics/docs/doj-2400-2.htm, which "sets forth the Department's policies and procedures regarding the solicitation and acceptance of gifts, devises and bequests of property of all kinds." The Order states that no Departmental employee may solicit a gift unless he or she has obtained the prior approval of the Attorney General or the Deputy Attorney General. DOJ Order 2400.2 ¶ 3.a.(1). Solicitations are rare and approved in only extraordinary circumstances.

In addition, the Assistant Attorney General for Administration (AAG/A) has the exclusive authority to accept "gifts made to the Department" or any of the Department's components. *Id.* ¶ 3.b.(1). Before accepting any gift, the AAG/A must consider whether: (1) the gift is appropriate for use; (2) the conditions the donor has placed on acceptance or use, if any, are "acceptable;" (3) any employee solicited the gift, and if so, whether approval was obtained; and (4) whether acceptance is "appropriate and advisable," in light of conflict-of-interest and ethics guidelines, including whether acceptance would "create the appearance of impropriety." *Id.* ¶ 3.b.(2).

The AAG/A has delegated to component heads the authority to determine whether to accept certain case-specific gifts from private parties in criminal and civil investigations, prosecutions, and civil litigation that have a value of $50,000 or less. The component head for U.S. Attorneys' Offices is the Director of the Executive Office for United States Attorneys. The component head may

accept the first offer from a source up to $50,000. A second or subsequent offer in the same fiscal year from the same source must be submitted to the AAG/A for approval when the value combined with the first gift exceeds $50,000. Gifts that are not case-specific, gifts of cash, gifts valued above $50,000, and extraordinary case-specific gifts continue to require approval by the AAG/A.

b. Distinction Between "Assistance" and "Gifts"

Historically, the Department has distinguished a gift from traditional forms of assistance provided by citizens during a criminal or civil investigation, prosecution, or civil litigation. Matters that constitute "assistance" are not gifts and, accordingly, are not subject to the procedures applicable to gifts. If the offered resource constitutes assistance, it may be accepted without approval, but if it is a gift, it cannot be accepted without obtaining approval as described later in this Chapter.

Law enforcement agencies routinely receive wide-ranging aid from private parties in the investigation and prosecution of federal crimes. Such aid has played an important and accepted role in the criminal process. *See, e.g., Commonwealth v. Ellis*, 708 N.E.2d 644, 651 (Mass. 1999) ("It is in the public interest that victims and others expend their time, efforts, and resources to aid public prosecutors."); *see also Wilson v. Layne*, 526 U.S. 603, 611-12 (1999) (noting that the use of third parties during the execution of a warrant to identify stolen property "has long been approved by this Court and our common-law tradition"). Victims and other private parties are often in a unique position to provide information and other aid in an investigation and litigation. Such private cooperation not only is desirable, but often is critical to law enforcement and the government's mission. In this vein, the vast majority of case-specific aid from private parties, particularly from victims and related parties, constitutes assistance and is not a gift.

A victim provides assistance when it offers services, equipment, or logistical support that enhances the efficiency of the government's efforts in relation to a case. Apart from cost savings, an offer of assistance enhances the Department's efficiency when the offer gives an added benefit that is unique because of the victim or related party's involvement. Assistance generally will be distinguishable in some way from what the Department could obtain through commercial obligations. For example, use of a victim company's office space to conduct interviews of witnesses constitutes assistance since that location provides accessibility to staff that would not be possible in a hotel or other location.

On the other hand, a victim company's offer to Departmental employees of its fleet of cars for local transportation, even if made in the course of a case, provides only a convenience that is no different from what the Department would obtain on the commercial rental market, and should not be accepted.

i. Assistance from Victims and Related Parties

Aid provided by a victim will generally be classified as assistance, rather than a gift. Examples of actions that constitute assistance when provided by a victim include:

- Providing factual or expert information in an investigation, or fact or expert testimony at trial
- Turning over the fruits of an internal investigation (e.g., collecting and analyzing financial or transactional data)
- Consulting with law enforcement during the investigation (e.g., reviewing seized evidence to distinguish legitimate copyrighted works from forgeries, identifying proprietary information in a trade secrets prosecution, or instructing professional staff and contractors to respond to queries from Departmental employees regarding technical subjects)
- Permitting agents to use equipment, services, or logistical support in circumstances where such assistance provides a unique benefit not available on the commercial market, such as the use of office space for employee interviews, surveillance, or document review
- Providing certain goods or services for use in the investigation or a related undercover operation (e.g., a bank providing credit card accounts in a credit card fraud investigation involving that bank)

Aid provided by a party that is related to the victim ("related party") will also generally constitute assistance. Related parties consist of those parties that have a close association with the victim and a shared interest with the victim in providing the particular assistance. Related parties can include a victim's immediate family, an industry association, or agents or contractors hired by the victim. For example, a computer security firm hired by a victim to monitor its computer network would be a related party in a case that involved the victim's computer network.

In certain circumstances, an entity may be an "indirect victim" of a crime and also be in a unique position to offer assistance. For example, an owner of an apartment building would be an indirect victim of a tenant who used his rental apartment to sell and deliver controlled substances. In addition, a

package delivery company that suspects use to transport and deliver illegal goods is also an indirect victim. Aid offered by an indirect victim generally will be considered assistance. For example, the landlord described above provides assistance with free use of an apartment for surveillance, as does the package delivery company when it provides its truck and uniform for an undercover agent to make a controlled delivery. However, depending on the value of the aid offered, and the potential appearance of impropriety that correlates to the value of the offer, an indirect victim's offer may cross the line from being permissible assistance to a gift that requires specific consideration before acceptance. For example, a landlord's offer of free use of an apartment for one year that has a market value of $25,000 in rent constitutes a gift.

ii. Private Investigators

Corporate victims and trade associations often retain private investigators to gather evidence to be used in a civil lawsuit or for referral to law enforcement authorities. Private investigators are in the class of "related parties" who may provide assistance to the Department. Intellectual property owners often outsource security and investigative responsibilities to other entities on an ongoing basis. In these cases especially, private investigators regularly turn up evidence of criminality and share it with law enforcement. Moreover, their investigative responsibilities do not end with the referral to authorities, as their clients expect them to continue to uncover evidence in related or separate matters, especially when the infringement or theft is committed by organized groups.

Several principles should guide the acceptance of assistance from private investigators. First, prosecutors and agents should not direct or advise an entity or individual in its private investigation before a referral is made to law enforcement authorities. Apart from issues regarding the acceptance of gifts versus assistance, activity by a private investigator may be imputed to the government for Fourth Amendment, entrapment, or other purposes, depending on the extent to which government officials direct or control those activities. Second, prosecutors and agents may not relinquish control of investigative responsibilities to private investigators after the Department has initiated an investigation. Third, if the private investigator continues (post-referral) to investigate the case or related matters and turns up additional evidence or information, employees may accept the continued assistance, but should be careful to avoid the appearance of implicit approval or direction. In fact, attorneys and other employees should evaluate whether the parallel

private investigation would interfere with the criminal matter and if so, whether the victim and private investigator should be asked to immediately cease any further investigation after the referral is made.

There may, however, be instances when a private investigator is in a unique position to assist the Department. If the investigator's assistance is within the scope of the work for which he was originally retained by the victim, the government may accept his assistance while he remains employed by the victim, and without payment from the Department. For example, if a private investigator has developed expertise in identifying the victim's property, or genuine products, he may assist in examining materials to determine whether they have been stolen from the victim or are counterfeit. If a private investigator made controlled buys of counterfeit products from a suspect prior to referring the case to a federal agency, and the Department believes a federally supervised controlled transaction is warranted, the private investigator may continue to assist the Department at the victim's expense if his involvement is needed to conduct the transaction and it is within the scope of the work for which he was originally retained.

iii. Cash

A direct contribution of money to the government to help fund the costs of law enforcement activities, either generally or in a particular case or cases, will almost always be a gift, not assistance. The private funding of federal law enforcement activities traditionally has not been considered assistance, and such direct funding raises serious ethical and other concerns, and would not be accepted by the Department. *See, e.g., People v. Eubanks*, 927 P.2d 310 (Cal. 1996) (victim paying cost of experts working for the district attorney's office created an actual conflict of interest). *But see Commonwealth v. Ellis*, 708 N.E.2d 644 (Mass. 1999) (funding of prosecution costs by insurance association permitted because authorized by statute). To the extent cash is used for mission-related functions, the Department may not augment its resources in this manner.

There is one exception to the principle that a direct contribution of money is an impermissible gift. When the government serves as a conduit for funds from the victim (or a related party) that are used for the purchase of the victim's stolen property, the payment of ransom, or a similar demand, the government's receipt of those funds does not constitute a gift. Accordingly, when an IP crime victim or a related party provides a Departmental employee funds to purchase

the victim's stolen property or pirated goods, the government is serving as a conduit for the funds and the funds are considered assistance. In these circumstances, the goods must be returned to the victim after completion of the government's case. Similarly, the government serves as a conduit when it uses funds from a victim or a related party to pay ransom or extortion on behalf of the victim. The Department has an established practice of accepting funds in these circumstances.

iv. Storage Costs in Counterfeit or Infringing Products Cases

A company that owns intellectual property has a significant independent interest in keeping counterfeit or infringing goods out of the stream of commerce. If federal law enforcement has seized offending products, it is likely that the victim would seek to impound and destroy the offending articles even if prosecution were declined. *See* 15 U.S.C. §§ 1116(d)(1)(A), 1118 (allowing for court-authorized seizure and destruction of trademark-infringing articles at the rights holder's request); 17 U.S.C. § 503 (allowing court to authorize impoundment and destruction of copyright-infringing articles and instrumentalities). When a victim has sought a court's approval to seize and retain counterfeit or infringing products and chooses to do so, the Department may accept the offer of "assistance" to store offending articles that may also be relevant to the Department's investigation.

There also may be instances when the victim will not choose to seek court approval of authority to retain and destroy illegal goods, yet offers the Department free storage at its facilities or elsewhere while the Department's case is pending. It generally is permissible to accept such an offer. However, depending on the amount of time and space used for storage, the company's offer to pay for storage may cross the line from being permissible assistance to an impermissible gift if the market value of the storage space is so exorbitant that continuing to accept free storage could raise a question of an appearance of impropriety. In such circumstances, a Department employee should consult with the assigned attorney and the employee or attorney's Deputy Designated Agency Ethics Official (DDAEO) before continuing to accept the free use of storage space.

v. Resources Donated for Ongoing Use by Law Enforcement

Resources provided by a victim or related party will generally be considered to be a gift if their use is *not* restricted to the investigation(s) or prosecution(s) in which the provider is a victim or related party. For example, a package delivery

company that gives the government free use of one of its delivery trucks for an undercover operation to investigate the hijacking of its trucks provides assistance. In contrast, the company's offer to the government of free use of its trucks for any undercover operation, regardless of the subject matter of the investigation, constitutes a gift. Similarly, a computer company that provides computers for the government to use in investigating and prosecuting the theft of trade secrets from that company gives assistance. But if the company permits the government to use those computers for additional purposes unrelated to that case, either for continued use after its conclusion or for an unrelated matter, the computers become a gift.

As a general rule, "assistance" is provided by a victim or related party for use in an investigation or litigation involving that person or entity. However, there may be limited circumstances in which a third party provides aid that is unique and not available on the open market in much the same way as a victim or related party's assistance. For example, the DEA and FBI have longstanding, ongoing relationships with private package delivery companies that are akin to assistance. During an investigation, the DEA and FBI sometimes execute controlled deliveries of packages that contain illegal goods. Given safety, evidentiary, and other concerns, an agent will use the company's truck and uniform rather than have the package delivery company and its employee perform this task. Of course, the delivery company uniforms and vehicles are not available on the open market. Yet their appearance is what is expected by the recipient, and it, therefore, provides the Department unique access to and identification of the intended recipient. The agent (in the package delivery uniform) may need to arrest the recipient of the package at the time of delivery. Given these unique and multiple factors, this type of aid is considered assistance.

vi. Assistance from Private Third Parties

The distinction between "assistance" and "gift" is also critical in cases involving resources donated by a private third party—that is, any person or entity that is neither a victim nor a related party. If the assistance provided by the third party is uniquely necessary to provide relevant information to the investigators, grand jury, judge, or jury, then it should generally be treated as assistance. If not, then it should generally be treated as a gift.

In many cases this determination will be simple. The most fundamental and traditional types of aid that citizens have always provided in criminal investigations and prosecutions—such as answering agents' and prosecutors'

questions, identifying suspects, and providing factual information and testimony—constitute assistance. This includes not only factual information gathered from individual citizens but also information that corporations and others provide from their records and databases. For example, an airline might provide information from passenger manifests, or a credit history service might provide credit information. Even though these activities may involve a cost to the third party in terms of time, effort, and expense and may provide a material benefit to the government, no one would suggest that such cooperation constitutes a gift; it is simply one of the responsibilities of citizenship.

In dealing with assistance provided by third parties, it may be helpful to consider whether the assistance could be obtained by compulsory process. For example, if the information could be obtained by grand jury subpoena without cost, it should not be considered to be a gift merely because the cooperating third party elects to volunteer the required information rather than be compelled by legal process to produce it.

The Department also may receive offers of free or reduced-fee consultation and testimony by experts or consultants. Individuals may be interested in sharing their expertise without a fee for a variety of reasons. Some experts or consultants may see the opportunity to testify on behalf of the United States, and be qualified as an expert, as a substantial benefit to their curriculum vitae or resume. In addition, an expert may charge an exorbitant market rate for his services to the general public that the Department cannot afford, and therefore, the expert may offer services for a reduced fee.

The Department may accept free expert or consultative services under its gift acceptance authority, 28 U.S.C. § 524(d), or 5 U.S.C. § 3109. Both statutes provide separate mechanisms to accept these services. Neither statute, however, obviates the necessity for Departmental attorneys and staff to assess whether it is appropriate to accept the services for free. The same issues that govern the propriety of acceptance of items apply to the offer of consultative services and testimony. An attorney in consultation with an agent or other employee and the DDAEO must decide whether free expert services are appropriate to accept, and whether the government's impartiality may or will be questioned in these circumstances.

For additional examples of what constitutes traditional assistance or a gift, please refer to Appendix J, which examines a variety of hypothetical offers of resources.

c. *Departmental Procedures for the Solicitation and Acceptance of Gifts and Assistance*

i. Consultative Process for Acceptance of Assistance and Gifts

A law enforcement officer or Department employee who receives any offer of assistance by a victim, related party, or witness beyond traditional assistance or access to company records should consult with the AUSA or Main Justice attorney who is assigned to the case or, if none, agency counsel, *and* the DDAEO who provides advice either to the law enforcement officer (or employee's) component or the attorney's office and component. The agent or employee in consultation with the appropriate counsel and DDAEO may determine that the offer is one of assistance (rather than a gift), and acceptance is appropriate. Disagreement among employees regarding these determinations should be submitted to the relevant component head(s) or designee and the Departmental Ethics Office, Justice Management Division (DEO) for resolution. Again, the component head for U.S. Attorneys' Offices is the Director of the Executive Office for United States Attorneys.

ii. Solicitation of Gifts

No Department employee may solicit gifts or encourage the solicitation of gifts to the Department unless the solicitation has been approved in advance by the Attorney General or the Deputy Attorney General. Solicitations will rarely be appropriate and, accordingly, rarely approved. There may, however, be unusual circumstances in which it would be appropriate to solicit a gift to the Department in connection with a particular investigation, prosecution, or litigation. In that instance, the appropriate office first should consult with the DEO, and then present the matter to the Office of the Deputy Attorney General for a determination.

iii. Acceptance of Gifts

Any gift of goods or services accepted from a private party in connection with a criminal or civil investigation, prosecution, or litigation must be approved in accordance with procedures set forth below. Except in extraordinary circumstances, that approval must be obtained before the gift is accepted. If approval cannot be obtained before the gift is accepted, approval must be obtained no later than seven days after acceptance.

- **Certain gifts may be accepted only by the AAG/A.**

Only the AAG/A may approve acceptance of a gift of goods or services that is valued in excess of $50,000. If a component or office is uncertain whether a gift is valued in excess of $50,000, it may consult with the DEO regarding the reasonable value of the gift. If an office cannot determine adequately whether a gift exceeds $50,000 in value, approval must be obtained from the AAG/A.

The AAG/A also must approve gifts of cash and gifts that are not case-specific, including gifts that will be used by the Department for purposes in addition to or after the conclusion of a particular investigation, prosecution, or litigation.

- **The AAG/A has delegated his authority to accept gifts from private parties for use by the Department in connection with a criminal or civil investigation, prosecution, or litigation.**

Component heads have been delegated authority to approve for their components the acceptance of a gift from a private party to be used in connection with a criminal or civil investigation, prosecution, or litigation that is (1) case-specific and (2) has a value of $50,000 or less. Component heads may further delegate this authority to one other individual at the Deputy Assistant Attorney General (or equivalent) level within his or her component.

- **Approval of acceptance must be coordinated among the relevant offices.**

If a law enforcement agent or other non-attorney employee receives an offer of a gift, that employee must notify and consult with an attorney, if any, who is assigned to the matter. The attorney, in conjunction with his or her component head, will determine whether to accept the offer. If no attorney has been assigned, the investigating component may decide whether to accept the offer of the gift. If an attorney from more than one office, Board, or Division is assigned a matter (e.g., an AUSA and attorney in the Criminal Division), both relevant component heads (or designees) must concur in the recommendation to accept a gift before it may be accepted. Disagreement among component heads may be resolved, upon request, by the AAG/A.

Component heads must ensure that a Gift Donation Form and a Gift Acceptance Form are completed for each gift acceptance approved by their respective component. The completed forms must be forwarded to Property

Management Services, Facilities and Administration Services Staff, Justice Management Division.

Any questions regarding gift issues should be directed to the DEO.

2. Professional Responsibility Issues

Several specific professional responsibility rules are implicated when the government accepts either assistance or gifts from outside parties. For ease of discussion, we refer here to the ABA Model Rules of Professional Conduct (*available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html), but note that a different set of professional conduct rules may apply, depending on the circumstances of each case and the rules in the attorney's state of licensure.

First, a prosecutor represents the United States and has a duty of confidentiality to that client. Rule 1.6(a) requires a lawyer to protect confidential client information and prohibits disclosure of such information unless impliedly authorized, or the client consents, or some other enumerated exception applies. The prohibition applies to privileged information, "matters communicated in confidence by the client [and] also to all information relating to the representation, whatever its source." Rule 1.6 cmt. [3]. When an investigator is hired or paid for by a victim to assist on a case and is working with government agents, the privately paid investigator might naturally expect to obtain information from the government in return for information he or she has disclosed to the government. However, a prosecutor must limit disclosures made about the case by him or herself and by the agents. *See* Rule 5.3(b), (c) (requiring lawyer to take reasonable steps to ensure that the conduct of non-lawyer assistants is compatible with the professional obligations of the lawyer and holding lawyer responsible for the noncompliance of non-lawyer assistants in some circumstances). Some disclosures may be impliedly authorized, while others would require the consent of the client; in most instances the United States Attorney or the Assistant Attorney General (or his or her designee) would provide the necessary consent for the United States. Of course, there are other limits on sharing of confidential grand jury information under Fed. R. Crim. P. 6(e).

When a prosecutor plans to disclose confidential information to the persons providing assistance or gifts, the attorney should seek written agreement from the person that he or she will not use or disclose the information except in

relation to the case without the express written consent of the appropriate official within the Department of Justice. Also, the prosecutor should consider whether sharing privileged information would waive the privilege.

The rules may require that assistance by third parties be disclosed to the court and/or to the defense, either to ensure that all representations to the court are accurate and complete, Rule 3.3 (candor toward the tribunal), or to clarify when the assistance or gifts provided by a private party might be seen as affecting the credibility of an important government witness, Rule 3.8(d) (special responsibilities of a prosecutor).

Moreover, there may be conflict of interest issues to resolve under Rule 1.7(a)(2), which recognizes that a lawyer may have a conflict of interest if "there is a significant risk that the representation of one or more clients will be materially limited by the lawyer's responsibilities to ... a third person or by a personal interest of the lawyer." In these circumstances, a lawyer may nevertheless represent the client if the client gives informed written consent. The United States Attorney or the Assistant Attorney General (or his or her designee) would have the authority to provide consent to the attorney's work on a case notwithstanding the conflict. One could imagine a scenario in which a continuing relationship with a victim/witness who is providing assistance in one case might raise concerns about the lawyer's representation of the United States in that or another case, particularly one involving the victim/witness.

Other professional conduct issues may arise because of assistance and gifts provided to the government. Each issue will require individual analysis, and questions may be directed to the Professional Responsibility Officer (PRO) in each office or to the Department's Professional Responsibility Advisory Office (PRAO).

3. Strategic and Case-Related Issues

Even if the resources offered by the victim or related parties are acceptable under both gift laws and policies and the rules of professional responsibility, an attorney must still consider whether accepting the assistance will adversely affect the case. Just because it might be permissible to accept an offer of either assistance or a gift does not make it advisable to do so in all instances. Depending on the scope, nature, or value of the assistance or gift, the public may question the Department's impartiality. Assistance that is extensive, unusual, or is, in fact or perception, of significant monetary value is more likely to raise questions

about the Department's impartiality and independence than assistance or a gift that is more discreet, of modest value, and routine.

The government must exercise independent and impartial judgment in the conduct of all criminal and civil matters. *See Young v. United States ex rel. Vuitton et Fils S.A.*, 481 U.S. 787, 803 (1987) ("The United States Attorney is the representative not of an ordinary party to a controversy, but of a sovereignty whose obligation to govern impartially is as compelling as its obligation to govern at all ....") (quoting *Berger v. United States*, 295 U.S. 78, 88 (1935)). When working with victims and other private parties, a Departmental employee must be aware that an entangled or intimate relationship with a private party can negatively affect a matter and the standing or respect accorded the Department. For example, a highly-paid, aggressive private investigator could be portrayed as a bounty hunter willing to entrap a defendant. The government might be portrayed as a pawn of wealthy corporate interests. The defense might claim that the victim's investigators were agents of the government and thereby seek to impute their conduct to the government for Fourth Amendment or entrapment purposes. The defense might seek to dismiss the case based on a claim of prosecutorial misconduct or conflict of interest. These questions or doubts can affect the Department's ability to successfully prosecute or litigate a matter.

An employee should consider, among other things, whether the offeror has an independent reason to offer the gift or assistance. Especially in parallel civil and criminal investigations, the fact that the victim would prefer to pay for expenses deemed important to the victim in pursuit of its civil claim tends to reduce the likelihood that a conflict of interest will be found. *See Hambarian v. Superior Court*, 44 P.3d 102, 109 (Cal. 2002) (finding no conflict presented by prosecution's use of a victim-retained consultant hired by the victim to support an anticipated civil suit).

An employee also should consider who the donor is. If the donor is an industry leader, the employee should avoid actions that appear to create a competitive advantage for that entity. If the donor is a trade association or combination of affected entities that is involved in ongoing monitoring or investigation to protect the industry as a whole, the offer may be considered more impartial. *See Commonwealth v. Ellis*, 708 N.E.2d 644, 649 (Mass. 1999) (explaining that likelihood of influence on a prosecutor's charging decisions is reduced when the resources are devoted to investigating industry-wide offenses rather than for the benefit of one particular victim).

The acceptance of donated resources is most problematic for courts when the resources are provided directly to the prosecutor or prosecutorial entity. *See People v. Eubanks*, 927 P.2d 310, 322-23 (Cal. 1997) (holding district attorney disqualified, and state attorney general substituted, after victim paid an invoice submitted to the prosecutor for expert services, among other expenses); *cf. Young v. United States ex rel. Vuitton et Fils S.A.*, 481 U.S. at 809 (holding that private counsel representing the beneficiary of a court order cannot be appointed to prosecute the defendant for violating the order). The less direct the benefit to the prosecution, the less likely the defendant will be able to obtain relief. *See Marshall v. Jerrico, Inc.*, 446 U.S. 238 (1980) (finding no realistic possibility that prospect of institutional benefit would unfairly influence decision to impose civil penalties by a Department of Labor administrator functioning as a prosecutor); *Calderon v. Superior Court of California*, No. C 97-1448 MJJ, 2001 WL 940904, at *7-8 (N.D. Cal. 2001) (finding victim's contribution of resources to police investigation unlikely to influence prosecutor's decisions). However, for the reasons discussed more fully herein, although a court may distinguish when aid is offered directly to a prosecutor or prosecutorial entity, as compared to an investigator or law enforcement agent, this distinction is not determinative for purposes of assessing whether the offer should be accepted in the first instance.

In addition, the Department's acceptance of a single, extraordinary gift from a victim or related party may impact the public, or more specifically, a jury's, perception of the Department's motivations and activities. If it appears that the Department's actions are influenced heavily by a private party, the Department's litigating posture and the public's respect will be weakened. A jury may vote against the Department's position because it perceives the Department is acting on behalf of a private party rather than as a representative of the United States' interests. In extreme cases, a court may conclude that the Department's acceptance of a gift created a conflict of interest and impaired the prosecutor's independence. *Cf. Eubanks*, 927 P.2d at 322. Of course, the standard of appropriate behavior is not whether a matter will be dismissed, but whether the appearance of impropriety or the lack of independence outweighs the benefit of the proffered gift or assistance. The Department, by its actions, must maintain the public's confidence in and respect for the criminal process, and the Department's reputation for fairness generally.

A Justice Department employee needs to balance the need for, or importance of, the aid against any negative perception by a jury or the public

that can influence adversely a particular case. Employees should evaluate whether the assistance or gift is likely to call into question their independence and impartiality, or create an appearance of impropriety. This analysis does not lend itself to clear or measured parameters. The decision whether to accept assistance or a gift often can involve difficult and nuanced issues. Given the potential ramifications, these decisions should be made through the consultative process among law enforcement personnel, other investigators, and attorneys before the matter is resolved. The trial attorney is in the best position to assess these concerns, and he must be consulted before any employee may accept an offer of resources. The assigned attorney also should consult with an ethics officer to determine whether the offer constitutes assistance or a gift that may be accepted under the gift procedures, and the offer conforms with the rules of professional responsibility.

4. Help and Advice

Each component (including each United States Attorney's Office) has qualified specialists to provide guidance, including a DDAEO who can provide advice on gift and assistance issues. The General Counsel's Office of the Executive Office for United States Attorneys provides guidance to U.S. Attorneys' offices on matters of government ethics, including recusal, outside employment and conflicts of interest. The office number is (202) 252-1600. Department employees also may seek guidance from the Departmental Ethics Office, Justice Management Division. The office number is (202) 514-8196.

For professional responsibility advice, an Assistant United States Attorney may first consult his or her supervisor and office Professional Responsibility Officer or seek advice from the Professional Responsibility Advisory Office (PRAO) at (202) 514-0458.

Appendix A
Commonly Charged Intellectual Property Crimes

This overview provides the elements, defenses, penalties, and sentencing guideline sections concerning most of the intellectual property crimes and alternative charges discussed in this Manual, as well as an index indicating which section of the Manual that discusses each crime.

Trafficking in Counterfeit Trademarks, Service Marks, or Certification Marks

18 U.S.C. § 2320(a)

Chapter III

Elements

1. That the defendant trafficked, attempted to traffic, [or, for offenses committed on or after December 31, 2011, conspired to traffic], in [goods] [services] [labels, documentation, or packaging for goods or services]

   [on or after December 31, 2011, includes counterfeit military good or service the use, malfunction, or failure of which is likely to cause serious bodily injury or death, the disclosure of classified information, impairment of combat operations, or other significant harm to a combat operation, a member of the Armed Forces, or to national security]

   [on or after July 9, 2012, includes a "counterfeit drug," as defined by 21 U.S.C. 321(g)]
2. That such trafficking, attempt to traffic, [or, on or after December 31, 2011, conspiracy to traffic] was intentional
3. That the defendant knowingly used a counterfeit mark on or in connection with the [goods] [services] [labels, documentation, or packaging for goods or services] in which the defendant trafficked, attempted to traffic, [or, on or after December 31, 2011, conspired to traffic]
4. That the use of the counterfeit mark was likely to cause confusion, to cause mistake, or to deceive

Counterfeit mark: "[A] spurious mark--(i) that is used in connection with trafficking in any goods, services, labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature; (ii) that is identical with, or substantially indistinguishable from, a mark registered on the principal register in the United States Patent and Trademark Office and in use, whether or not the defendant knew such mark was so registered; (iii) that is applied to or used in connection

with the goods or services for which the mark is registered with the United States Patent and Trademark Office, or is applied to or consists of a label, patch, sticker, wrapper, badge, emblem, medallion, charm, box, container, can, case, hangtag, documentation, or packaging of any type or nature that is designed, marketed, or otherwise intended to be used on or in connection with the goods or services for which the mark is registered in the United States Patent and Trademark Office; and (iv) the use of which is likely to cause confusion, to cause mistake, or to deceive; or ... a spurious designation that is identical with, or substantially indistinguishable from, a designation as to which the remedies of the Lanham Act are made available by reason of section 220506 of title 36."

Defenses

Overrun goods: Had authorization but exceeded it (i.e., authorized to make 1,000 copies but made 5,000).

Gray market goods: Goods legitimately manufactured and sold overseas and then imported into U.S. outside traditional distribution channels.

Repackaging genuine goods: Genuine goods repackaged with genuine marks or reproduced marks, with no intent to deceive or confuse.

Statutory maximum penalties

First offense: 10 years' imprisonment and fine of $2,000,000 or twice the gain/loss (individual); fine of $5,000,000 or twice the gain/loss (organization); for violations involving counterfeit military goods or services and counterfeit drugs, 20 years' imprisonment and a fine of up to $5 million (individual) and $15 million (organization); enhanced penalties may also be available under § 2320(b)(2) if a defendant knowingly or recklessly causes or attempts to cause serious bodily harm or death by any of the offenses listed in § 2320(a)

Subsequent offense: 20 years' imprisonment and $5,000,000 fine or twice the gain/loss (individual); $15,000,000 fine or twice the gain/loss (organization); for violations involving counterfeit military goods or services and counterfeit drugs, 30 years' imprisonment and a fine of $15 million (individual) and $30 million (organization)

Guideline section: United States Sentencing Guideline § 2B5.3

Criminal Copyright Infringement (Felony & Misdemeanor)

17 U.S.C. § 506(a) & 18 U.S.C. § 2319

Chapter II

Elements for prosecutions under subsections 506(a)(1)(A) and (a)(1)(B)

1. That the works that the defendant is alleged to have [reproduced] [distributed] were protected by copyright
2. That the defendant infringed the copyrights of the works by [reproducing] [distributing to the public] one or more copies of [each of] the copyrighted works
3. That the defendant willfully infringed the copyrights [and]
4. That the defendant, during a 180-day period, reproduced or distributed ten (10) or more copies of one or more copyrighted works which have a total retail value of more than $2,500 [and]

[5. [optional] That the act of infringement was for the purpose of commercial advantage or private financial gain]

Elements for prosecutions under subsection 506(a)(1)(C)

1. That copyrights exist for the works that the defendant is alleged to have distributed
2. That the defendant infringed the copyrights of the works by distributing to the public one or more copies of [each of] the copyrighted works
3. That the defendant willfully infringed the copyrights
4. That the works distributed by the defendant were being prepared for commercial distribution
5. That the defendant knew or should have known that the works were intended for commercial distribution [and]
6. That the defendant distributed the works by making them available on a computer network accessible to members of the public [and]

[7. Optional: That the act of infringement was for the purpose of commercial advantage or private financial gain]

Elements for Misdemeanor Copyright Infringement

Elements 1, 2 & 3 are the same as the base felony elements except that any infringement of the copyright is covered, not just infringement by reproduction or distribution.

4. The defendant i®nfringed EITHER
   (a) for purposes of commercial advantage or private financial gain, (17 U.S.C. § 506(a)(1)(A) & 18 U.S.C. § 2319(b)(3)); OR
   (b) by reproduction or distribution of one or more copyrighted works with a total retail value of more than $1,000 within a 180-day period, (17 U.S.C. § 506(a)(1)(B) & 18 U.S.C. § 2319(c)(3)).

Defenses

First sale: The first purchaser and any subsequent purchaser of a specific lawfully made copy of a copyrighted work may sell, display (privately), or dispose of their copy, but may not reproduce and distribute additional copies made from that work.

Fair use: Allows otherwise infringing use of a work for purposes such as (but not limited to) criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research.

Archival exception for computer software: Owner of a copy of a computer program may copy the program as necessary to use the program or do machine maintenance or repair, and as an archival backup, subject to certain limitations.

Statutory maximum penalties

17 U.S.C. § 506(a)(1)(A)

First offense: 5 years' imprisonment and fine of $250,000 or twice the gain/loss (individual); fine of $500,000 or twice the gain/loss (organization)

Subsequent offense: 10 years' imprisonment and fine of $250,000 or twice the gain/loss (individual); fine of $500,000 or twice the gain/loss (organization)

17 U.S.C. § 506(a)(1)(B)

First offense: 3 years' imprisonment and fine of $250,000 or twice the gain/loss (individual); fine of $500,000 or twice the gain/loss (organization)

Subsequent offense: 6 years' imprisonment and fine of $250,000 or twice the gain/loss (individual); fine of $500,000 or twice the gain/loss (organization)

17 U.S.C. § 506(a)(1)(C)

First offense: Same as § 506(a)(1)(A) if purpose was for commercial advantage or private financial gain; if not, same as § 506(a)(1)(B)

Misdemeanor: 1 year's imprisonment and fine of $100,000 or twice the gain/loss

Guideline section: United States Sentencing Guideline § 2B5.3

Unauthorized Recording of a Motion Picture (Camcording)

18 U.S.C. § 2319B

Chapter II, Section F.

Elements

1. That the defendant used, or attempted to use, an audiovisual recording device to transmit or make a copy of a motion picture or other audiovisual work from a performance of such work in a motion picture facility, specifically [describe use or attempted use]
2. That such use, or attempted use of the device, was done knowingly
3. That such use, or attempted use of the device, was without the authorization of the copyright owner
4. That [describe motion picture or audiovisual work] is protected by copyright

Statutory maximum penalties

First offense: 3 years' imprisonment and fine of $250,000 or twice the gain/loss (individual); fine of $500,000 or twice the gain/loss (organization)

Subsequent offense: 6 years' imprisonment and fine of $250,000 or twice the gain/loss (individual); fine of $500,000 or twice the gain/loss (organization)

Guideline section: United States Sentencing Guideline § 2B5.3

Trafficking in Illicit Labels or Counterfeit Labels, Documentation or Packaging for Copyrighted Works

18 U.S.C. § 2318

Chapter VI

Elements

1. That the defendant trafficked in

   [labels affixed to/enclosing/accompanying/ designed to be affixed to, to enclose, to accompany] [*describe work/ documentation/ packaging*;]

   [documentation/packaging]
2. That the

   [labels were counterfeit/illicit]

   [documentation/packaging was counterfeit]
3. That the defendant acted knowingly
4. Federal jurisdiction is satisfied because:

   the offense occurred in special maritime territories or other areas of special jurisdiction of the United States;

   the offense used or intended to use the mail or a facility of interstate or foreign commerce;

   the counterfeit or illicit labels were affixed to, enclosed, or accompanied copyrighted materials (or were designed to); or

   the documentation or packaging is copyrighted.

Statutory maximum penalties

5 years' imprisonment and fine of $250,000 or twice the gain/loss (individual); fine of $500,000 or twice the gain/loss (organization)

Guideline section: United States Sentencing Guideline § 2B5.3

Trafficking in Recordings of Live Musical Performances (Bootlegging)

18 U.S.C. § 2319A

Chapter II, Section F.

Offense

Whoever, without the consent of the performer or performers involved, knowingly and for purposes of commercial advantage or private financial gain—

(1) fixes the sounds or sounds and images of a live musical performance in a copy or phonorecord, or reproduces copies or phonorecords of such a performance from an unauthorized fixation;

(2) transmits or otherwise communicates to the public the sounds or sounds and images of a live musical performance; or

(3) distributes or offers to distribute, sells or offers to sell, rents or offers to rent, or traffics in any copy or phonorecord fixed as described in paragraph (1), regardless of whether the fixations occurred in the United States.

Statutory maximum penalties

First offense: 5 years' imprisonment and fine of $250,000 or twice the gain/loss (individual); fine of $500,000 or twice the gain/loss (organization)

Second offense: 10 years' imprisonment and fine of $250,000 or twice the gain/loss (individual); fine of $500,000 or twice the gain/loss (organization)

Guideline section: United States Sentencing Guideline § 2B5.3

Digital Millennium Copyright Act

(Anti-Circumvention and Anti-Trafficking)

17 U.S.C. §§ 1201(a)(1), 1201(b)(1), 1204(a)

Chapter V

Elements for Unauthorized Circumvention of Access Controls

1. The defendant acted willfully
2. The defendant circumvented a technological measure
3. The technological measure effectively controls access (i.e., access control)
4. The access control was to a copyrighted work
5. The act of circumvention was for the purpose of commercial advantage or private financial gain

Elements for Trafficking in Access Control Circumvention Tools

1. The defendant acted willfully
2. The defendant manufactured, imported, offered to the public, provided, or otherwise trafficked in any technology, product, service, device, component, or part thereof
3. The technology, product, service, device, component, or part thereof either: (A) was primarily designed or produced for the purpose of, (B) has only limited commercially significant purpose or use other than, or (C) was marketed by that person or another acting in concert with that person with that person's knowledge for use in, circumventing protection afforded by a technological measure
4. The defendant acted for commercial advantage or private financial gain

Defenses

Regulatory: The Librarian of Congress promulgates regulatory exemptions every three years that apply only to § 1201(a)(1)(A)'s prohibitions against circumventing access controls.

Certain nonprofit entities: Nonprofit libraries, archives, educational institutions, or public broadcasting entities exempted from criminal prosecution in many cases.

Information security: "[A]ny lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee" or contractor of the federal government or a state government is exempt from all three of § 1201's prohibitions for information security work on "government computer, computer system, or computer network."

Reverse engineering and interoperability of computer programs: Three reverse engineering or "interoperability" defenses for individuals using circumvention technology are provided by statute. These defenses are limited to computer programs.

Encryption research: Activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products.

Restricting minors' access to Internet: Courts may waive violations of subsections 1201(a)(1)(A) and 1201(a)(2) to allow parents to protect their children from inappropriate material available on the Internet, or to prohibit manufacturers from producing products designed to enable parents to protect their children.

Protection of personally identifying information: Circumventing an access control to disable files that collect personally identifiable information.

Security testing: No violation of § 1201(a)(1)(A) occurs if testing does not constitute copyright infringement or a violation of other applicable law such as the Computer Fraud and Abuse Act of 1986.

Statutory maximum penalties

First offense: 5 years' imprisonment and fine of $500,000 or twice the gain/loss

Second offense: 10 years' imprisonment and $1,000,000 fine or twice the gain/loss

Guideline section: United States Sentencing Guideline § 2B5.3

Theft of Trade Secrets

18 U.S.C. § 1832

Chapter IV

Elements

1. The defendant knowingly misappropriated information (e.g., possessed, stole, transmitted, downloaded) (or conspired or attempted to do so)
2. The defendant knew or believed this information was proprietary and that he had no claim to it
3. The information was in fact a trade secret (unless conspiracy or an attempt is charged)
4. The defendant intended to convert the trade secret to the economic benefit of anyone other than the owner
5. The defendant knew or intended that the offense would injure the owner of the trade secret
6. The trade secret was related to a product or service used or intended for use in interstate or foreign commerce

Defenses

Parallel development: Defendants discovered information underlying a trade secret through their own independent efforts.

Reverse engineering: Defendants discovered information underlying a trade secret by taking a thing that incorporates the trade secret apart to determine how it works or how it was made or manufactured.

Impossibility: Impossibility is no defense to charges of attempt or conspiracy.

Advice of counsel: May negate mens rea.

Claim of right—public domain and proprietary rights: Mens rea might be negated if defendant believed in good faith that he had a right to use the information, either because it was in the public domain or because it belonged to him.

Trade secret: All forms and types of financial, business, scientific, technical, economic, or engineering information, if (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information

derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

Secrecy: Courts required to take any action necessary to protect the confidentiality of the trade secret during litigation.

Statutory maximum penalties

> 10 years' imprisonment and fine of $250,000 or twice the gain/loss (individual); $5,000,000 fine or twice the gain/loss (organization)

Guideline section: United States Sentencing Guideline § 2B1.1

Economic Espionage

18 U.S.C. § 1831

Chapter IV

Elements

1. The defendant knowingly misappropriated information (e.g., possessed, stole, transmitted, downloaded) (or conspired or attempted to do so)
2. The defendant knew or believed this information was proprietary and that he had no claim to it
3. The information was in fact a trade secret (unless conspiracy or an attempt is charged)
4. The defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality, or foreign agent

Defenses: See **Theft of Trade Secrets** (18 U.S.C. § 1832)

Pre-Indictment Approval Required

Statutory maximum penalty

15 years' imprisonment and fine of $5,000,000 or twice the gain/loss (individual); $10,000,000 fine or three times the value of the stolen trade secret, including expenses for research and design and other costs of reproducing the trade secret, or twice the gain/loss (organization)

Guideline section: United States Sentencing Guideline § 2B1.1

Unauthorized Access of a Computer

18 U.S.C. § 1030(a)(2), (a)(4)

Chapter IV, Section F.

Offense under § 1030(a)(2)—Unlawfully accessing or attempting to access a computer to obtain information

Whoever intentionally accesses [or attempts to access] a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*)

(B) information from any department or agency of the United States OR

(C) information from any protected computer

Protected computer: a computer (i) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (ii) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States

Enhancement pursuant to 18 U.S.C. § 1030(c)(2)(B)

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000.

Statutory maximum penalty

1 year's imprisonment and fine of $100,000

Enhanced statutory maximum penalties

5 years' imprisonment (second offense: 10 years' imprisonment) and fine of $250,000 or twice the gain/loss (individual); fine of $500,000 or twice the gain/loss (organization)

Guideline section: United States Sentencing Guideline § 2B1.1

Offense under § 1030(a)(4)—Unlawfully accessing or attempting to access a protected computer to further a fraud

Whoever knowingly and with intent to defraud, accesses [or attempts to access] a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

Statutory maximum penalties

5 years' imprisonment and fine of $250,000 or twice the gain/loss (first offense), 10 years' imprisonment and fine of $250,000 or twice the gain/loss (second offense)

Guideline section: United States Sentencing Guideline § 2B1.1

Interstate Transportation, Sale, or Receipt of Stolen Property

18 U.S.C. §§ 2314, 2315

Chapter II, Section F. & Chapter IV, Section F.

Transportation offense under § 2314

> Whoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud; or
>
> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transports or causes to be transported, or induces any person or persons to travel in, or to be transported in interstate or foreign commerce in the execution or concealment of a scheme or artifice to defraud that person or those persons of money or property having a value of $5,000 or more ....

Sale or receipt offense under § 2315

> Whoever receives, possesses, conceals, stores, barters, sells, or disposes of any goods, wares, or merchandise, securities, or money of the value of $5,000 or more, or pledges or accepts as security for a loan any goods, wares, or merchandise, or securities, of the value of $500 or more, which have crossed a State or United States boundary after being stolen, unlawfully converted, or taken, knowing the same to have been stolen, unlawfully converted, or taken ....

Statutory maximum penalties

> 10 years' imprisonment and fine of $250,000 ($500,000 for organizations) or twice the gain/loss

Guideline section: United States Sentencing Guidelines §§ 2B1.1, 2B1.5

Mail and Wire Fraud Statutes

18 U.S.C. §§ 1341, 1343, 1346

Section F. of Chapters II, III, IV, and VI

Mail Fraud Offense Under § 1341

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or to sell, dispose of, loan, exchange, alter, give away, distribute, supply, or furnish or procure for unlawful use any counterfeit or spurious coin, obligation, security, or other article, or anything represented to be or intimated or held out to be such counterfeit or spurious article, for the purpose of executing such scheme or artifice or attempting so to do, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or deposits or causes to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing ....

Wire Fraud Offense Under § 1343

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice ....

Theft of Honest Services Under § 1346

> [T]he term "scheme or artifice to defraud" includes a scheme or artifice to deprive another of the intangible right of honest services.

Statutory maximum penalties

> 20 years' imprisonment and fine of $250,000 or twice the gain/loss (individual); fine of $500,000 or twice the gain/loss (organization)

If affecting a financial institution or in relation to any benefit paid in connection with a presidentially declared major disaster or emergency: 30 years' imprisonment and fine of $1,000,000 or twice the gain/loss

Guideline section: United States Sentencing Guideline §§ 2B1.1, 2C1.1

Prohibition on Devices to Intercept Communications

18 U.S.C. § 2512

Offense

Any person who intentionally—

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce ....

Statutory maximum penalties

5 years' imprisonment and fine of $250,000 ($500,000 for organizations) or twice the gain/loss

Guideline section: United States Sentencing Guideline § 2H3.2

Unauthorized Reception of Cable Service

47 U.S.C. § 553

Chapter II, Section F.

Offense

> No person shall [willfully] intercept or receive or assist in intercepting or receiving any communications service offered over a cable system, unless specifically authorized to do so by a cable operator or as may otherwise be specifically authorized by law.

Enhancement: Done for purposes of commercial advantage or private financial gain

Statutory maximum penalties for willful violation

> 6 months' imprisonment and fine of $1,000

Enhanced penalties

> 2 years' imprisonment (5 years' for subsequent offense) and fine of $50,000 ($100,000 for subsequent offense)

Guideline section: United States Sentencing Guideline § 2B5.3

Trafficking in Satellite Decryption Devices

47 U.S.C. § 605(e)(4)

Chapter II, Section F.

Offense

Any person who manufactures, assembles, modifies, imports, exports, sells, or distributes any electronic, mechanical, or other device or equipment, knowing or having reason to know that the device or equipment is primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite services ....

Statutory maximum penalties

5 years' imprisonment and fine of $500,000 or twice the gain/loss

Guideline section: United States Sentencing Guideline §§ 2B5.3, 2H3.1

Appendices B-F Sample Indictments and Jury Instructions

Appendix B. Copyright Infringement

http://dojnet.doj.gov/criminal/ccips/online/2319.htm

Appendix C. Trademark Counterfeiting

http://dojnet.doj.gov/criminal/ccips/online/2320.htm

Appendix D. Theft of Trade Secrets and Economic Espionage

http://dojnet.doj.gov/criminal/ccips/online/1831_1832.htm

Appendix E. Digital Millennium Copyright Act

http://dojnet.doj.gov/criminal/ccips/online/DMCA.htm

Appendix F. Trafficking in Counterfeit or Illicit Labels and Counterfeit Documentation and Packaging

http://dojnet.doj.gov/criminal/ccips/online/2318.htm

Appendix G
Intellectual Property Contact List

1. **Federal Law Enforcement Contacts**
2. **Federal International Contacts**
3. **Trademark Organization Contacts**
4. **Copyright Organization Contracts**
5. **Other Organization Contacts**

1. Federal Law Enforcement Contacts

Computer Crime and Intellectual Property Section (CCIPS)
Criminal Division, U.S. Department of Justice
1301 New York Avenue NW, Suite 600
Washington, DC 20530
Tel: 202-514-1026
Fax: 202-514-6113
http://www.cybercrime.gov

Prosecution of, and guidance, support, resources, and materials for prosecuting domestic and international criminal IP offenses; development of IP enforcement policy; and support and oversight of the federal prosecution of IP crimes.

National Intellectual Property Rights Coordination Center
Homeland Security Investigations
2451 Crystal Drive, STOP 5105
Arlington, VA 20598
Tel: 866-IPR-2060
Fax: 703-603-3872
Email: IPRcenter@dhs.gov
http://www.iprcenter.gov

The IPR Center is a task force that brings together the key U.S. agencies involved in federal criminal enforcement of IPR laws. The IPR Center partners include: U.S. Immigration and Customs Enforcement's Homeland Security Investigations, U.S. Customs and Border Protection; Federal Bureau of Investigation; Food and Drug Administration's Office of Criminal Investigations; U.S. Postal Inspection Service; Defense Criminal Investigative Service; U.S. Patent and Trademark Office; and Nuclear Regulatory Commission.

Federal Bureau of Investigation
Intellectual Property Rights Center
Unit Chief
2451 Crystal Drive
Arlington, VA 22202
Tel: 703-603-3962
Fax: 703-603-3899
http://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr

Responsible for all IPR and Internet fraud investigations; support and oversight of the FBI's IPR enforcement program.

Department of Homeland Security (DHS)
Customs and Border Protection (CBP)
1300 Pennsylvania Avenue NW
Washington, DC 20229
http://www.cbp.gov

- Office of International Trade—Trade Policy and Programs—IPR Policy and Programs Division
  Tel: 202-863-6091
  Fax: 202-863-6520
  Email: iprpolicyprograms@dhs.gov

  Coordinates with rights holders, members of the trade community, CBP offices, other federal agencies, and foreign governments, in developing and implementing IPR strategy, policy, and programs.

- Office of International Trade—Regulations and Rulings—IPR and Restricted Merchandise Branch
  Tel: 202-325-0093
  Tel: 202-325-0020
  Fax: 202-325-0120
  Email: hqiprbranch@dhs.gov

  Administers and advises on legal components and aspects of the agency's IPR enforcement programs, issues rulings and infringement determinations, manages recordation system.

- IPR E-Recordation (IPRR) Application
  Email: iprr.questions@dhs.gov
  https://apps.cbp.gov/e-recordations/

  Online application for IP owners to record their trademarks and copyrights with CBP to protect against the importation of infringing products. Regulations and Rulings—IPR and Restricted Merchandise Branch, listed above, is the point of contact for any questions regarding recordation.

- Office of Trade Relations
  Tel: 202-344-1440
  Fax: 202-344-2064
  Email: traderelations@dhs.gov
  http://www.cbp.gov/xp/cgov/toolbox/contacts/otr_contacts.xml

  Liaison between industry and CBP. Reviews concerns voiced by individuals or trade groups and furnishes recommendations to resolve justified complaints.

U.S. Postal Inspection Service
Mail Fraud Group
475 L'Enfant Plaza SW
Washington, DC 20260
Tel: 202-268-4267
Tel: 1-877-876-2455
Fax: 202-268-7316
https://postalinspectors.uspis.gov

Support and oversight of Postal Inspection Service's mail fraud enforcement nationwide, including investigation of IP crimes committed by use of the mails.

Food and Drug Administration (FDA)
Office of Criminal Investigations
7500 Standish Place, Suite 250N
Rockville, MD 20855
Tel: 240-276-9500
Fax: 240-276-8368
http://www.fda.gov/oci/

Conducts and coordinates criminal investigations of suspected violations of the Federal Food, Drug, and Cosmetic Act (FDCA), to include cases involving counterfeit, adulterated and misbranded FDA regulated products, as well as violations of the Federal Anti-Tampering Act (FATA); and other related Title 18 statutes.

Consumer Product Safety Commission (CPSC)
4330 East West Highway
Bethesda, MD 20814
Tel: 301-504-7923; 800-638-2772
Fax: 301-504-0124
http://www.cpsc.gov

Has jurisdiction over approximately 15,000 types of consumer products, including coffee makers, electrical cords, toys, baby seats and cribs. Investigates leads into possible hazardous products; develops voluntary standards with industry, issues and enforces mandatory standards; and bans products if no feasible standard will adequately protect the public.

Internet Crime Complaint Center (IC3)
1 Huntington Way
Fairmont, WV 26554
Tel: 800-251-3221; 304-363-4312; complaint center: 800-251-7581
Fax: 304-363-9065
http://www.ic3.gov

Partnership between National White Collar Crime Center (NW3C) and FBI. Allows victims to report fraud over the Internet; alerts authorities of suspected criminal or civil violations; offers law enforcement and regulatory agencies a central repository for complaints related to Internet fraud.

2. Federal International Contacts

U.S. Department of Justice

- **International Coordinator in Each U.S. Attorney's Office**
  Office of International Affairs, Department of Justice
  Tel.: 202-514-0000
- **Computer Crime & Intellectual Property Section**
  Tel.: 202-514-1026
- **Office of International Affairs, Department of Justice**
  Legal Attaché program
  Tel.: 202-514-0000
- **Office of Overseas Prosecutorial Development & Training**
  Resident Legal Advisor program
  Tel.: 202-514-1323
- **Federal Bureau of Investigation Legal Attaché Program**
  http://www.fbi.gov/contact/legat/legat.htm

U.S. Trade Representative's List of Nations that Fail to Provide Adequate IP Protection
Annual Special 301 Report
http://www.ustr.gov/trade-topics/intellectual-property

3. Trademark Organization Contacts

United States Patent and Trademark Office (USPTO)
Director of the USPTO
P.O. Box 1450
Alexandria, VA 22313-1450
Tel.: 800-786-9199
Email: usptoinfo@uspto.gov
http://www.uspto.gov/

The USPTO is the Federal agency for granting U.S. patents and registering trademarks. The USPTO advises the President of the United States, the Secretary of Commerce, and U.S. Government agencies on IP policy, protection, and enforcement; and promotes stronger and more effective IP protection around the world. To obtain a copy of a certified trademark registration:

- Email: dsd@uspto.gov
  Fax: Public Records at 571-273-3250
  Telephone number for information or inquiries:
  Tel: 571-272-3150 or 800-972-6382

International AntiCounterfeiting Coalition (IACC)
Robert C. Barchiesi
President
1730 M Street NW, Suite 1020
Washington, DC 20036
Tel.: 202-223-6667
Fax: 202-223-6668
Email: iacc@iacc.org
http://www.iacc.org

The touchstone of the IACC's mission is to combat counterfeiting and piracy by promoting laws, regulations and directives designed to render the theft of IP undesirable and unprofitable. It is comprised of a cross section of business and industry - from autos, apparel, luxury goods and pharmaceuticals, to food, software and entertainment - affected by counterfeiting.

International Trademark Association (INTA)
Candice Li
External Relations Manager, Anti-Counterfeiting
655 Third Avenue, 10th Floor
New York, NY 10017-5617
Tel.: 212-642-1739
Fax: 212-768-7796
http://www.inta.org

INTA is a global not-for-profit association of over 5,900 trademark owners, professionals, and academics dedicated to supporting trademarks and

related IP in order to protect consumers and to promote fair and effective commerce.

4. Copyright Organization Contacts

Library of Congress Copyright Office
Certifications & Documents
LM 402
101 Independence Avenue SE
Washington, DC 20559
Tel.: 202-707-6787
http://www.loc.gov/

Retains files of registered copyrights and unpublished works; provides information on obtaining copies of copyright registrations.

Association of American Publishers (AAP)
M. Lui Simpson
Executive Director
International Copyright Enforcement and Trade Policy
455 Massachusetts Avenue NW, Suite 700
Washington, DC 20001
Tel.: 202-347-3375, ext. 541
Fax: 202-347-3690
http://www.publishers.org

AAP is the national trade association of the U.S. book publishing industry. AAP's more than 300 members include most of the major commercial publishers in the United States, as well as smaller and non-profit publishers, university presses and scholarly societies. AAP members publish hardcover and paperback books in every field, educational materials for the elementary, secondary, postsecondary, and professional markets, scholarly journals, computer software, and electronic products and services.

Business Software Alliance (BSA)
Jon Berroya
Director, Global Internet Enforcement
20 F Street NW, Suite 800
Washington, DC 20001
Tel.: 202-872-5500
Fax: 202-872-5501
http://www.bsa.org

BSA is a global association of software industry leaders, which runs a comprehensive set of programs to expand legal software markets in the world. BSA assists in identifying and locating victims, identifying and valuing infringing products; technical assistance with copyright protection technologies; assists in obtaining copyright registration certificates.

Entertainment Software Association (ESA)
575 7th Street NW, Suite 300
Washington, DC 20004
Tel.: 202-223-2400
Fax: 202-223-2401
Email: esa@theESA.com
http://www.theESA.com

Represents companies that publish video and computer games for video consoles, personal computers and the Internet. Assists in identifying and locating victims, identifying and valuing infringing products; technical assistance with copyright and copyright protection technologies; assists in obtaining copyright registration certificates.

The Independent Film & Television Alliance (IFTA)
Susan Cleary
Vice President & General Counsel
10850 Wilshire Boulevard, 9th Floor
Los Angeles, CA 90024-4321
Tel.: 310-446-1000
Fax: 310-446-1600
http://www.ifta-online.org/

Represents the independent motion picture and television industry.

International Federation of the Phonographic Industry (IFPI)
Jeremy Banks
Director, Anti-Piracy
IFPI Secretariat
10 Piccadilly
London
W1J 0DD
United Kingdom
Tel.: 011-44-207-878-6804
Email: info@ifpi.org
http://www.ifpi.org/

Represents the worldwide recording industry's international organizations, legal strategies, litigation, and public relations. Coordinates international strategies in anti-piracy enforcement, technology, and lobbying of governments. IFPI and the Recording Industry Association of America (RIAA) work closely together. RIAA recommends contacting it before contacting the IFPI.

International Intellectual Property Alliance (IIPA)
1818 N Street NW, 8th Floor
Washington, DC 20036
Tel.: 202-355-7900
Fax: 202-355-7899
http://www.iipa.com

IIPA is a private sector coalition of seven U.S. trade associations representing U.S. copyright-based industries in bilateral and multilateral efforts working to improve international protection and enforcement of copyrighted materials and open up foreign markets closed by piracy and other market access barriers.

Motion Picture Association of America (MPAA)
Michael Robinson
EVP Content Protection
Chief of Operations
Motion Picture Association of America
15301 Ventura Boulevard, Building E
Sherman Oaks, CA 91403

Tel.: 818-995-6600
Fax: 818-285-4403
http://www.mpaa.org

Represents the film and entertainment industry. Assists in identifying and locating victims, identifying and valuing infringing products; technical assistance with copyright and copyright protection technologies; assists in obtaining copyright registration certificates.

Recording Industry Association of America (RIAA)
L. Carlos Linares, Jr., Esq.
Vice President, Anti-Piracy Legal Affairs
1025 F Street NW, 10th Floor
Washington, DC 20004
Tel.: 202-775-0101
Fax: 202-775-7253
http://www.riaa.org

Represents the United States recording industry. Assists in identifying and locating victims, identifying and valuing infringing products; technical assistance with copyright and copyright protection technologies; assists in obtaining copyright registration certificates.

Software & Information Industry Association (SIIA)
1090 Vermont Avenue NW, 6th Floor
Washington, DC 20005-4095
Tel.: 202-289-7442
Fax: 202-289-7097
http://www.siia.net

Keith Kupferschmid
General Counsel and Senior Vice President, Intellectual Property
Tel.: 202-789-4442
Email: keithk@siia.net

SIIA represents software companies and publishers of magazines, books, newspapers, databases and other digital publications. SIIA's mission is to protect, promote, and inform the software and content industry. Assists in identifying and locating victims, identifying and valuing infringing

products; technical assistance with copyright and copyright protection technologies; assists in obtaining copyright registrations.

5. Other Organization Contacts

Aerospace Industries Association (AIA)
Kirsten Koepsel
Director, Legal Affairs & Tax
1000 Wilson Boulevard, Suite 1700
Arlington, VA 22209
Tel: 703-358-1044
Fax: 703-358-1144
http://www.aia-aerospace.org

Represents the aerospace, defense, and space industries. Assist members in working with governmental bodies to put rules in place regarding the protection of IP; assist in processes to seek relief and remedies; assist members in civil and criminal instances to ensure consistent responses to governmental bodies.

Global Intellectual Property Center (GIPC)
1615 H Street, NW
Washington, DC 20062
Tel: 202-463-5601
Fax: 202-463-3114
Email: gipc@uschamber.com
http://www.theglobalipcenter.com

Established in 2007 as an affiliate of the U.S. Chamber of Commerce, the GIPC works to raise awareness and increase support among key audiences for the value of strong IP rights, to promote and defend robust and effective IP rights and norms, and to strengthen the protection and enforcement of IP in the U.S. and abroad.

Intellectual Property Owners Association (IPO)
Herbert C. Wamsley
Executive Director
1501 M Street, NW, Suite 1150
Washington, DC 20005
Email: info@ipo.org
Tel.: 202-507-4500
Fax: 202-504-4501
http://www.ipo.org

Established in 1972, IPO represents owners of patents, trademarks, copyrights and trade secrets. It is the only association in the U.S. that serves all IP owners in all industries and all fields of technology. IPO advocates effective and affordable IP ownership rights and concentrates on: supporting member interests relating to legislative and international issues; analyzing current IP issues; providing information and educational services; and disseminating information to the general public on the importance of IP rights.

Motor & Equipment Manufacturers Association (MEMA)
1030 15th Street NW, Suite 500 East
Washington, DC 20005
Tel: 202-393-6362
Fax: 202-737-3742
http://www.mema.org

Catherine Boland
Vice President, Legislative Affairs
Tel.: 202-312-9241
Email: cboland@mema.org

Dan Houton
Director, Government Relations
Tel: 202-312-9250
Email: dhouton@mema.rog

Represents more than 1000 companies that manufacture motor vehicle components and systems. MEMA, in conjunction with its affiliate associations, created the Brand Protection Committee (BPC) to help

address and set the association's priorities in the areas of counterfeiting, diversion, non-compliant products and IP rights.

National Association of Manufacturers (NAM)
733 10th Street NW, Suite 700
Washington, DC 20001
Tel: 202-637-3000
Fax: 202-637-3182
Email: manufacturing@nam.org
http://www.nam.org

Represents 11,000 manufacturing companies in every industrial sector and in all 50 states. Responsible for anti-counterfeiting and anti-piracy policy initiatives, and worldwide IP rights protection.

Pharmaceutical Security Institute
Thomas T. Kubic
President and CEO
8100 Boone Blvd., Suite 220
Vienna, VA 22182
Tel.: 703-848-0160
Fax: 703-848-0164
Email: psi@psi-inc.org
http://www.psi-inc.org/

Collects, analyzes, and disseminates information about the counterfeiting, illegal diversion and theft of pharmaceuticals in support of enforcement efforts worldwide. Its membership includes 25 pharmaceutical manufacturers from many nations.

Appendix H
Checklist for Reporting an Intellectual Property Crime

This checklist serves as a guide for the type of information that would be helpful for a victim or a victim's authorized representative to include when reporting an intellectual property violation to law enforcement. Victims are encouraged to complete the checklist prior to making a report, if possible. Prosecutors and/or investigators may also use the checklist as a framework to gather information from victims. The checklist contains two sections: one intended for use in criminal copyright and trademark cases (including counterfeit trademarks, certification marks or service marks), and the other intended for use in criminal trade secret cases. They can be adapted for use in other intellectual property offenses as well.

Criminal Copyright and Trademark Infringement

- ✓ Background / Contact Information
- ✓ Description of the Intellectual Property
- ✓ Description of the Intellectual Property Crime
- ✓ Origin and Entry (If Applicable)
- ✓ Possible Suspects
- ✓ Internet Involvement
- ✓ Civil Enforcement Proceedings

Criminal Trade Secret Offenses

- ✓ Note on Confidentiality
- ✓ Background / Contact Information
- ✓ Description of the Trade Secret
- ✓ Measures Taken to Protect the Physical Trade Secret Location
- ✓ Confidentiality and Non-Disclosure Agreements
- ✓ Electronically-Stored Trade Secrets
- ✓ Document Controls
- ✓ Employee Controls
- ✓ Description of the Trade Secret's Misappropriation
- ✓ Civil Enforcement Proceedings

Criminal Copyright and Trademark Infringement

1. Background and Contact Information

- ❑ Victim's Name:
- ❑ Primary Address:
- ❑ Nature of Business:
- ❑ Primary Contact:
- ❑ Work Phone:
- ❑ Mobile Phone:
- ❑ Email:
- ❑ Fax:

2. Description of the Intellectual Property

- ❑ Describe the copyrighted material or trademark/service mark/certification mark (e.g., title of copyrighted work, identity of logo), including any factors that make its infringement especially problematic (e.g., threats to public health and safety, pre-release piracy).

- ❑ Is the work or mark registered with the U.S. Copyright Office or on the principal register of the U.S. Patent and Trademark Office?[1]
  ___ YES ___NO

If yes, please provide the following:

- ❍ Registration Date:
- ❍ Registration Number:

If no, state if and when you intend to register:

- ❑ Do you have a certified copy of the certificate of registration?
  ___ YES ___NO

[1] Registered trademarks can be found through the U.S. Patent & Trademark Office's searchable database at: http://tess2.uspto.gov/bin/gate.exe?f=tess&state=4010:lmjahh.1.1

- ❑ Is the work or mark recorded with U.S. Customs and Border Protection (CBP)?[2]
  ___ YES ___NO

  If yes, please provide the following:

  - ❍ Recordation Date:
  - ❍ Recordation Number:

- ❑ What is the approximate retail value of the infringed work, good, or service?

- ❑ Has the work or mark been the subject of a previous civil or criminal enforcement action? If so, please provide a general description as well as the case name, case number, and name of court.

3. Description of the Intellectual Property Crime

- ❑ Describe how the theft or counterfeiting was discovered.

- ❑ Do you have any examination reports of the infringing or counterfeit goods? ___YES ___NO

  If yes, please provide those reports to law enforcement. Please also provide a photograph or sample of the goods, if possible.

- ❑ Describe the type of infringement (e.g., manufacture, reproduction, import, export, distribution).

- ❑ Describe the scope of the infringing operation, including the following information:

  - ❍ Estimated quantity of illegal distribution:
  - ❍ Estimated value of illegal distribution:
  - ❍ Estimated time period of illegal distribution:

[2] IP rights holders can apply online at https://apps.cbp.gov/e-recordations/ to record their trademarks and copyrights with CBP to protect against the importation of infringing products.

- ❍ Is the illegal distribution national or international? Which states and/or countries?

- ❑ Identify where the infringement or counterfeiting occurred, and describe the location.

4. Origin and Entry (If Applicable)

- ❑ Identify the country of origin of the infringing item.

- ❑ Identify the date, location, and mode of entry into the United States.

- ❑ Identify the names of shippers and Harmonized Tariff Schedule designation and provide any other applicable shipping or customs information.

5. Possible Suspects

- ❑ Identify the name(s) or location(s) of possible suspects, including the following information:

  - ❍ Name (Suspect #1):
  - ❍ Phone number:
  - ❍ Email address:
  - ❍ Physical address:
  - ❍ Current employer, if known:
  - ❍ Any other identifiers:
  - ❍ Reason for suspicion:
  - ❍ Name (Suspect #2):
  - ❍ Phone number:
  - ❍ Email address:
  - ❍ Physical address:
  - ❍ Current employer, if known:
  - ❍ Any other identifiers:
  - ❍ Reason for suspicion:

6. Internet Involvement

- ❑ If the distribution of infringing or counterfeit goods involves the Internet, identify the following:
  - ❍ How the Internet is involved (e.g., websites, FTP, mail, chat rooms):
  - ❍ Relevant Internet address, including any affiliate websites (domain name, URL, IP address, email):
  - ❍ Login or password for website:
  - ❍ Operators of website, if known:
    - Location of the servers and website host:
    - Country where domain name is registered:
  - ❍ Has the right holder sent a cease and desist notice to the website? ___YES ___NO

    If yes, please provide the following:

    - Date of notice:
    - Do you have a copy of the notice? ___ YES ___NO

- ❑ If you have conducted an internal investigation into the theft or counterfeiting activities, please describe any evidence acquired and submit, if possible, any investigative reports.

7. Civil Enforcement Proceedings

- ❑ Have you ever received counterfeit goods from the target listed above? ___YES ___NO

- ❑ If yes, did you place the target on notice that the goods received were counterfeit?

- ❑ Has a civil enforcement action been filed against the suspects identified above? ___YES ___NO

  If yes, identify the following:

  - ❍ Name of court and case number:
  - ❍ Date of filing:

- ❍ Names of attorneys:
- ❍ Status of case:

If no, please state whether a civil action contemplated, what type and when.

- ❑ Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

Trade Secret Offenses

NOTE ON CONFIDENTIALITY

Federal law provides that courts "shall enter such orders and take such action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws." 18 U.S.C. § 1835. Prosecutors utilizing any of the information set forth below will generally request the court to enter an order to preserve the status of the information as a trade secret and prevent its unnecessary and harmful disclosure.

1. Background and Contact Information

- ❑ Victim's Name:
- ❑ Primary Address:
- ❑ Nature of Business:
- ❑ Primary Contact:
- ❑ Work Phone:
- ❑ Mobile Phone:
- ❑ Email:
- ❑ Fax:

2. Description of the Trade Secret

- ❑ Generally describe the trade secret (e.g., source code, formula, technology, process, device).

- ❑ Provide an estimated value of the trade secret using one or more of the methods listed below:

Estimated Value	Method
	Cost to develop the trade secret
	Acquisition cost (include date / source of acquisition)
	Fair market value if sold

❑ Provide the name, title and contact information of the person most knowledgeable about the trade secret's valuation:

3. Measures Taken to Protect the Physical Trade Secret Location

❑ Describe the company's general security practices concerning entry to and moving within its premises, such as fencing the perimeter of the premises, visitor control systems, using alarming or self-locking doors or security personnel.

❑ Describe any security measures the company has employed to prevent unauthorized viewing or access to the trade secret, such as locked storage facilities or "Authorized Personnel Only" signs at access points.

❑ Describe any protocol the company employs to keep track of employees accessing trade secret material such as sign in/out procedures for access to and return of trade secret materials.

❑ Are employees required to wear identification badges? ___YES ___ NO

❑ Does the company have a written security policy? ___YES ___NO

If yes, please provide the following information:

- ❍ Does the security policy address in any way protocols on handling trade secret information? ___YES ___NO
- ❍ How are employees advised of the security policy?
- ❍ Are employees required to sign a written acknowledgment of the security policy? ___YES ___NO

❑ The name, title, and contact information of the person most knowledgeable about matters relating to the security policy:

❑ How many employees have access to the trade secret?

❑ Was access to the trade secret limited to a "need to know" basis? ___YES ___NO

If yes, describe how "need to know" was maintained in any ways not identified elsewhere (e.g., closed meetings, splitting tasks between employees and/or vendors to restrict knowledge, etc.):

4. Confidentiality and Non-Disclosure Agreements

❑ Does the company enter into confidentiality and non-disclosure agreements with employees and third parties concerning the trade secret? ___YES ___NO

❑ Has the company established and distributed written confidentiality policies to all employees? ___YES ___NO

❑ Does the company have a policy for advising company employees regarding the company's trade secrets? ___YES ___NO

5. Electronically-Stored Trade Secrets

❑ If the trade secret is computer source code or other electronically-stored information, how is access regulated (e.g., are employees given unique user names, passwords, and electronic storage space, and was the information encrypted)?

- ❑ If the company stores the trade secret on a computer network, is the network protected by a firewall? ___YES ___NO

- ❑ Is remote access permitted into the computer network? ___YES ___NO

  If yes, is a virtual private network utilized? ___YES ___NO

- ❑ Is the trade secret maintained on a separate computer server? ___YES ___NO

- ❑ Does the company prohibit employees from using unauthorized computer programs or unapproved peripherals, such as high capacity portable storage devices? ___YES ___NO

- ❑ Does the company maintain electronic access records such as computer logs? ___YES ___NO

6. Document Controls

- ❑ If the trade secret consists of documents, were they clearly marked "CONFIDENTIAL" or "PROPRIETARY"? ___YES ___NO

- ❑ Describe the document control procedures employed by the company, such as limiting access and sign in/out policies.

- ❑ Was there a written policy concerning document control procedures? ___YES ___NO

  If yes, how were employees advised of it?

- ❑ Provide the name, title, and contact information of the person most knowledgeable about the document control procedures:

7. Employee Controls

- ❑ Are new employees subject to a background investigation? ___YES ___NO

- ❑ Does the company conduct regular training for employees concerning steps to safeguard trade secrets?___YES ___NO

- ❑ Does the company hold "exit interviews" to remind departing employees of their obligation not to disclose trade secrets? ___YES ___NO

8. Description of the Misappropriation of the Trade Secret

- ❑ Identify the name(s) or location(s) of possible suspects, including the following information:

    - ❍ Name (Suspect #1):
    - ❍ Phone number:
    - ❍ Email address:
    - ❍ Physical address:
    - ❍ Current employer, if known:
    - ❍ Any other identifiers:
    - ❍ Reason for suspicion:
    - ❍ Name (Suspect #2):
    - ❍ Phone number:
    - ❍ Email address:
    - ❍ Physical address:
    - ❍ Current employer, if known:
    - ❍ Any other identifiers:
    - ❍ Reason for suspicion:

- ❑ Describe how the misappropriation of the trade secret was discovered.

- ❑ Describe the type(s) of misappropriation (e.g., stealing, copying, drawing, photographing, downloading, uploading, altering, destroying, transmitting, receiving).

- ❑ Was the trade secret stolen to benefit a third party, such as a competitor or another business? ___YES ___NO

If yes, identify that business and its location.

- ❑ Do you have any information that the trade secret was stolen to benefit a foreign government or instrumentality of a foreign government?
  ___YES ___NO

  If yes, identify the foreign government or instrumentality and describe that information.

- ❑ If the suspect is a current or former employee, describe all confidentiality and non-disclosure agreements in effect.

- ❑ Identify any physical locations associated with the misappropriated trade secret, such as where it may be currently stored or used.

- ❑ If you have conducted an internal investigation into the misappropriation, please describe any evidence acquired and provide any investigative reports that you can.

9. Civil Enforcement Proceedings

- ❑ Has a civil enforcement action been filed against the suspects identified above? ___YES ___NO

  If yes, please provide the following information:

  - ❍ Name of court and case number:
  - ❍ Date of filing:
  - ❍ Names of attorneys:
  - ❍ Status of case:

  If no, please state whether a civil action was contemplated, what type and when.

- ❑ Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

Appendix I
Pre-PRO-IP Act Forfeiture Statutes for IP Offenses

Criminal Copyright Infringement

Administrative	
Infringing Items	**Yes.** • 17 U.S.C. § 509(b) (West 2007) (administrative forfeiture of infringing items forfeitable civilly). • 17 U.S.C. §§ 602-603 (West 2007) (forfeiture of *prohibited*[1] imports of infringing items). • 19 U.S.C. § 1595a(c)(2)(C) (CBP forfeiture of imports of infringing[2] items).
Facilitating Property	**Yes.** • 17 U.S.C. § 509(b) (West 2007) (permitting administrative forfeiture of facilitating property forfeitable civilly). • 19 U.S.C. § 1595a(a) (CBP forfeiture of property facilitating *importation* of infringing items).
Proceeds	**Yes.** • 18 U.S.C. § 981(d) (permitting administrative forfeiture of proceeds forfeitable civilly).
Civil	
Infringing Items	**Yes.** • 17 U.S.C. § 509(a) (West 2007). • 17 U.S.C. §§ 602-603 (West 2007).
Facilitating Property	**Yes.** • 17 U.S.C. § 509(a) (West 2007) (plates, molds, masters and other equipment used to make infringing copies).
Proceeds	**Yes.** • 18 U.S.C. § 981(a)(1)(C).

Criminal	
Infringing Items	**Yes (mandatory).** • 17 U.S.C. § 506(b) (West 2007) (*mandating* criminal forfeiture upon a criminal conviction). • 17 U.S.C. §§ 602-603 (West 2007). • 28 U.S.C. § 2461(c) (*permitting* criminal forfeiture of property forfeitable civilly).
Facilitating Property	**Yes (mandatory).** • 17 U.S.C. § 506(b) (West 2007). • 28 U.S.C. § 2461(c).
Proceeds	**Yes.** • 18 U.S.C. § 2461(c).

Digital Millennium Copyright Act

Administrative	**No.**
Civil	**No.**
Criminal	**No**.

Economic Espionage Act (Trade Secret Theft)

Administrative	
Contraband	**No.**
Facilitating Property	**No**.
Proceeds	**No.**
Civil	
Contraband	**No.**
Facilitating Property	**No.**
Proceeds	**No.**
Criminal	
Contraband	**No**.
Facilitating Property	**Yes.** • 18 U.S.C. § 1834(a)(2) (West 2007).
Proceeds	**Yes (mandatory).** • 18 U.S.C. § 1834 (a)(1) (West 2007).

Counterfeit/Illicit Labels, Documentation, and Packaging for Copyrighted Works

Administrative	
Counterfeit/Infringing Items	**Yes.** • 17 U.S.C. § 509(b) (West 2007). • 19 U.S.C. § 1595a(c)(2)(C) (CBP forfeiture of imports of infringing[3] items).
Facilitating Property	**Yes.** • 17 U.S.C. § 509(b) (West 2007). • 19 U.S.C. § 1595a(a) (CBP forfeiture of property facilitating *importation* of infringing items).
Proceeds	**Yes.** • 18 U.S.C. § 981(d) (permitting administrative forfeiture of proceeds forfeitable civilly).
Civil	
Counterfeit/Infringing Items	**Yes.** • 17 U.S.C. § 509(a) (West 2007).
Facilitating Property	**Yes.** • 17 U.S.C. § 509(a) (West 2007).
Proceeds	**Yes.** • 18 U.S.C. § 981(a)(1)(C).
Criminal	
Counterfeit/Infringing Items	**Yes (mandatory).** • 18 U.S.C. § 2318(d) (West 2007) (*mandating* criminal forfeiture upon a criminal conviction). • 28 U.S.C. § 2461(c) (*permitting* criminal forfeiture of property forfeitable civilly).
Facilitating Property	**Yes (mandatory).** • 17 U.S.C. § 2318(d) (West 2007). • 28 U.S.C. § 2461(c).
Proceeds	**Yes.** • 18 U.S.C. § 981(a)(1)(C). • 28 U.S.C. § 2461(c).

Unauthorized Fixations of Live Musical Performances ("Bootlegging")

Administrative	
Unauthorized Recordings	**Yes.** • 18 U.S.C. § 2319A(c). • 19 U.S.C. § 1595a(c)(2)(C) (CBP forfeiture of imports of infringing[4] items).
Facilitating Property	**Yes.** • 19 U.S.C. § 1595a(a) (CBP forfeiture of property facilitating *importation* of infringing items).
Proceeds	**Yes.** • 18 U.S.C. § 981(d) (permitting administrative forfeiture of proceeds forfeitable civilly).
Civil	
Unauthorized Recordings	**Yes.** • 18 U.S.C. § 2319A(c).
Facilitating Property	**No.**
Proceeds	**Yes.** • 18 U.S.C. § 981(a)(1)(C).
Criminal	
Unauthorized Recordings	**Yes (mandatory).** • 18 U.S.C. § 2319A(b) (West 2007) (*mandating* criminal forfeiture upon a criminal conviction). • 28 U.S.C. § 2461(c) (*permitting* criminal forfeiture of property forfeitable civilly).
Facilitating Property	**Yes (mandatory).** • 18 U.S.C. § 2319A(b) (West 2007) (plates, molds, matrices, masters, tapes and film negatives – discretionary as to additional equipment).
Proceeds	**Yes.** • 28 U.S.C. § 2461(c).

Unauthorized Recording of Motion Pictures ("Camcording")

Administrative	
Unauthorized Recordings	**Yes.** • 19 U.S.C. § 1595a(c)(2)(C) (CBP forfeiture of imports of infringing[5] items).
Facilitating Property	**Yes.** • 19 U.S.C. § 1595a(a) (CBP forfeiture of property facilitating *importation* of infringing items).
Proceeds	**No.**
Civil	
Unauthorized Recordings	**No.**
Facilitating Property	**No.**
Proceeds	**No.**
Criminal	
Unauthorized Recordings	**Yes (mandatory).** • 18 U.S.C. § 2319B(b) (West 2007).
Facilitating Property	**Yes (mandatory).** • 18 U.S.C. § 2319B(b) (West 2007).
Proceeds	**No.**

Goods, Services, Labels, Documentation, and Packaging with Counterfeit Marks

Administrative	
Counterfeit Items	**Yes.** • 18 U.S.C. § 2320(b)(2) (West 2007) (for offenses committed from March 16, 2006 through October 12, 2008). • 19 U.S.C. § 1595a(c)(2)(C) (CBP forfeiture of imports of infringing[6] items).
Facilitating Property	**Yes.** • 18 U.S.C. § 2320(b)(2) (West 2007) (for offenses committed from March 16, 2006 through October 12, 2008). • 19 U.S.C. § 1595a(a) (CBP forfeiture of property facilitating *importation* of infringing items).
Proceeds	**Yes.** • 18 U.S.C. § 981(d) (permitting administrative forfeiture of items forfeitable civilly).
Civil	
Counterfeit Items	**Yes (mandatory).** • 18 U.S.C. § 2320(b)(1)(A), (C) (West 2007) (for offenses committed from March 16, 2006 through October 12, 2008).
Facilitating Property	**Yes.** • 18 U.S.C. § 2320(b)(1)(B) (West 2007) (for offenses committed from March 16, 2006 through October 12, 2008).
Proceeds	**Yes.** • 18 U.S.C. § 981(a)(1)(C).

Criminal	
Counterfeit Items	**Yes (mandatory for offenses committed on or after March 16, 2006).** • 18 U.S.C. § 2320(b) (West 2005) (for offenses committed before March 16, 2006 – discretionary, and did not require a criminal conviction – the United States could obtain an order for the *destruction* of the items upon a preponderance of the evidence showing). • 18 U.S.C. § 2320(b)(3)(A)(iii) (West 2007) (for offenses committed from March 16, 2006 through October 12, 2008) (*mandatory* criminal forfeiture upon a criminal conviction). • 28 U.S.C. § 2461(c) (permitting criminal forfeiture of property forfeitable civilly).
Facilitating Property	**Yes (mandatory for offenses committed on or after March 16, 2006).** • 18 U.S.C. § 2320(b)(3)(A)(ii) (West 2007) (for offenses committed from March 16, 2006 through October 12, 2008). • 28 U.S.C. § 2461(c).
Proceeds	**Yes (mandatory for offenses committed on or after March 16, 2006).** • 18 U.S.C. § 2320(b)(3)(A)(i) (West 2007) (for offenses committed from March 16, 2006 through October 12, 2008). • 28 U.S.C. § 2461(c).

(Footnotes)
1 17 U.S.C. § 602(a) provides that unauthorized importation is an infringement merely if the copies or phonorecords "have been acquired outside the United States," even if they were lawfully manufactured abroad, and their importation may be enjoined by the rights holder, who enjoys the exclusive right to distribution within the United States. 17 U.S.C. § 602(b), however, provides that only *piratical* copies – those whose making "would have constituted an infringement of copyright if this title had been applicable" – are *prohibited* from importation and thus subject to administrative seizure and forfeiture under 17 U.S.C. § 603(c).

2 Like 17 U.S.C. § 603(c), 19 U.S.C. § 1595a(c)(2)(C) permits administrative seizure and forfeiture only of *piratical* copies – "merchandise or packaging in which copyright ... violations are involved (including, but not limited to, violations of ... section 506 of title 17, United States Code ...)."

3 19 U.S.C. § 1595a(c)(2)(C) permits administrative seizure and forfeiture of "merchandise or packaging in which copyright ... violations are involved (including, but not limited to, violations of ... section 2318 ... of title 18, United States Code ...)."

4 The theory would be that 19 U.S.C. § 1595a(c)(2)(C) permits administrative seizure and forfeiture of "merchandise or packaging in which copyright ... violations are involved," even though the statute does not cite specifically 18 U.S.C. § 2319A.

5 The theory would be that 19 U.S.C. § 1595a(c)(2)(C) permits administrative seizure and forfeiture of "merchandise or packaging in which copyright ... violations are involved," even though the statute does not cite specifically 18 U.S.C. § 2319B.

6 19 U.S.C. § 1595a(c)(2)(C) permits administrative seizure and forfeiture of "merchandise or packaging in which ... trademark ... violations are involved (including, but not limited to, violations of ... 15 U.S.C. 1124, 1125, or 1127 ... or section ... 2320 of title 18, United States Code) ....".

Appendix J
Examples of Traditional Assistance and Gifts to Law Enforcement

The examples below of what constitutes traditional assistance to law enforcement or a gift are based on the examples included with a memorandum issued by Deputy Attorney General Paul J. McNulty entitled *Guidance for Acceptance of Assistance and Gifts from Private Parties for Use in Connection with Investigations and Litigation* (May 2006). These examples highlight certain factors to consider and addresses the consultative process that should be followed. Please note that not every factor that should be considered has been identified below for each scenario. The examples are provided to highlight certain elements, but do not reflect the entire analysis.

1. ***Scenario*:** The Department has received information from a private investigator who has an ongoing contract with a motion picture association to investigate pirated and counterfeit goods, including pirated movie DVDs. The investigator provides information regarding websites and points of contact for persons/entities that may have a connection to the counterfeit materials.

   ***Analysis*:** This information constitutes traditional assistance; no particular consultation is required before a Departmental employee may accept this information.

   Continuing Scenario: The Department has initiated its own investigation based on the initial information provided by the association's private investigator. After the Department's investigation has begun, and without any further communications or direction from an FBI agent or the Criminal Division attorney assigned to the matter, the private investigator uncovers another source that appears to be involved with the counterfeit materials. The investigator reports this new information to the FBI agent.

Analysis: This information also constitutes traditional assistance that the FBI agent and attorney may accept. The attorney and agent may need to consult with each other to determine whether the investigator's efforts may interfere with the Department's activities, and whether the investigator should be advised to alter his activities in some manner in order to avoid any interference. Neither the agent nor attorney should advise the investigator what types of evidence are desired for the Department's investigation.

2. ***Scenario:*** A nationwide retail giant has its own security force and has spent considerable resources to set up its own forensics laboratory to fight shoplifting and other crimes against the company. The local FBI office is investigating a matter that has no connection to the retail company. The FBI office, however, believes that the equipment at the retail company's laboratory is superior to the Department's capabilities for enhancing photographs for identification. The FBI office solicits the retail giant for help, and the business readily agrees to provide forensic assistance without charge. The enhanced photograph allows the FBI to continue its investigation with greater efficiency.

   Analysis: Initially, the FBI must obtain prior approval from the Deputy Attorney General or the Attorney General before any representative may contact the retail company to seek its services. The free forensic services constitute a gift. Since the value of these services is less than $50,000, the agent and attorney must seek the component head's approval in order to accept these services for free. In considering this offer, the component head must consider why the Department is seeking outside forensics aid. The Department may need a third party's gift because the Department does not own or have at its disposal the same equipment. In addition, the time-sensitive nature of the case might require immediate action, and the Department might not gain access to such equipment with the same speed as that offered as a gift. In this situation, with advance approval of the solicitation the Department may accept the gift.

3. ***Scenario:*** Consider the same facts set forth in Scenario #2, but assume that the retail giant informed the local FBI office that it had a forensics laboratory with equipment capable of performing a variety of functions, and that it was offering general access to its equipment and staff for

investigative purposes any time that the Department determined the company's resources would benefit the Department.

Analysis: A retail giant's standing offer to allow the Department to use its forensic facilities, whether for case-specific matters or general investigative purposes, should be considered carefully. (Initially, this company's offer does not trigger the same considerations set forth in No. 2, where the Department solicited the gift.). As noted above, there may be instances when private industry has forensic resources that are not available to the Department, and the immediacy of the situation may warrant the Department's use of outside resources. However, the decision to use a third party's services is distinct from the decision to accept such services free of cost. In deciding whether to accept the services for free, counsel should consider whether there are any pending matters in the Department in which the retail giant is a party or could be affected directly by a particular matter.

One-time gifts of free assistance may be permissible. However, it is particularly important that the Department carefully scrutinize a third party's offer to use its services for free on multiple occasions or on a periodic basis for separate cases or matters (e.g., several times a year). The Department should be circumspect in accepting more than one gift from the same source within one fiscal year.

Again, while the donor may have resources unavailable to the Department, the Department should consider paying for the services provided. Even if the full cost is difficult to assess, the Department and a third party can identify a reasonable value for the unique services provided.

One reason for the Department's disinclination to accept multiple offers from one source is that the costs of pursuing the Department's mission must be fully identified and presented as part of its budget for Congress to accept or reject. Accepting free services that are critical to the Department's performance of its mission on a frequent or regular basis masks the actual costs of its annual operations. Second, periodic or regular acceptance of free services from an entity can raise an appearance of a conflict of interest, particularly if any matter later arises involving that donor.

The component head may accept the first offer from a source up to $50,000. A second or subsequent offer in the same fiscal year from the same source must be submitted to the Assistant Attorney General for Administration (AAG/A) for approval when the value combined with the first gift exceeds $50,000.

4. ***Scenario:*** A corporation's products are being counterfeited and its computer network has been infiltrated. The corporation has hired a computer security firm to evaluate the extent of the computer breach and to recommend modifications to its system. The corporation has told Departmental attorneys and investigators that it may speak with its employees and the computer security firm's personnel about the breach, and utilize their expertise as necessary. The corporation is paying for the computer security firm's services throughout the Department's investigation, including time spent meeting with Department employees. One computer firm employee has particular proficiency in computer programming, and he would be an expert witness in any litigation against the defendant to discuss the unauthorized access and damage to the corporation's security and computer privacy. The victim corporation also has provided office space for Departmental employees to interview corporate staff and the computer firm employees.

   Analysis: The corporation is a victim. The computer firm is a 'related party' because it is retained by the corporation. Access to both companies' personnel during the investigation is traditional assistance that does not warrant any formal approval process. The corporate and security firm employees are in a unique position to provide useful information on behalf of their employer/contractor. The agent and attorney should consult with each other, and potentially with the Professional Responsibility Officer (PRO) and the Deputy Designated Agency Ethics Official (DDAEO), to determine the extent to which they will accept the corporation's offers. Using corporate space for interviews does not raise any particular concerns. The computer security expert who assessed the damage to the corporation has distinct advantages over another computer expert who was not involved in the assessment. Despite this favorable position, the trial attorney should determine whether the potential appearance of the corporation's self-interest in paying for the expert witness' testimony does not outweigh the benefit of this expert's testimony before accepting the services.

5. ***Scenario:*** The DEA is investigating a suspect for selling and delivering drugs from his apartment. In order to enhance its surveillance and consistent with its investigative procedures, DEA wants to rent an apartment in the building where the suspect lives. DEA approaches the owner of the building and offers to pay market rent for an apartment. The owner has a vacant apartment in a desirable location to conduct surveillance in the building. The owner is supportive of the DEA's efforts and offers the apartment to DEA for three months free of charge. The fair market value of the vacant apartment is $1,500/month.

   Analysis: The owner is an indirect victim since the suspect's illegal activities have an adverse affect on the owner's property. Offers of aid from an indirect victim generally constitute assistance, although the value of the offer may be such that it should be considered a gift. Given the short time frame (three months) and the value involved ($4,500), this offer constitutes assistance, and an agent in consultation with an attorney may decide to accept the offer. However, if the owner offered the DEA agent free use of the apartment for nine months and that amount of time (or longer) was necessary for a more complex investigation, the agent and attorney should seek approval to accept the offer as a gift. Given that the owner is taking the apartment off the market for an extended period of time, the offer is more substantial than before, and higher-level approval (by the component head for a gift) is warranted. There is no clear line defining when assistance becomes a gift because of the financial value or imposition involved. For offers that exceed three months, an attorney should consult with the DDAEO to determine whether the offer may be accepted as assistance, or considered a gift.

6. ***Scenario:*** The Criminal Division is investigating a highly technical computer crimes case. A university professor has conducted research in the narrow field at issue. A Criminal Division attorney contacted the professor for general background information on this issue, saying that the Department is willing to pay for his consultative services. The professor is willing to provide advice, assistance, and testimony in federal court for free. Although the professor has no prior experience as a witness, the attorney intends to proffer the professor as an expert.

Analysis: The professor is a third party and he has offered the attorney a gift. Assuming that the number of hours to prepare and present testimony is limited, the value of the professor's services will be below $50,000. Although the Department (and component's budget) will always benefit from no-cost expert services, it is not always appropriate to accept this type of offer. While the professor will benefit professionally from his 'expert' qualification, this intangible benefit does not necessarily mean the Department should avoid the costs of payment. The attorney should consult with the PRO and DDAEO to determine the appropriate course of action.

7. ***Scenario:*** The FBI is investigating the sale of counterfeit goods. The corporate maker of the true product has offered to give the FBI $1 million to purchase the counterfeit goods from an identified broker. The FBI, in consultation with the local United States Attorney's Office, accepts the offer, and makes arrangements with the corporation to provide the $1 million. The counterfeit goods are purchased. The corporation arranged for the goods to be transported and stored in its warehouse pending its initiation of a civil proceeding.

   Analysis: Because the Department is serving as the conduit for cash to recover counterfeit materials, the Department may accept the victim's offer of funds for this particular purpose. The agent should seek approval from the AUSA prior to accepting the victim's funds. Because the cost of storage to the company at its own facilities is minimal, the Department may accept the company's offer to store the goods at the victim's expense.

8. ***Scenario:*** An industry leader in the computer field has developed a software program that can meld various databases and enhance search capabilities for the law enforcement community. The company has offered this program to the Department. While it is not available for sale to the public, the program (including the technical support to assist its operations) is valued over $800,000.

   Analysis: Given the high value, this offer must be submitted to the AAG/A for acceptance. Moreover, more concerns arise because this program would enhance the Department's general capabilities, and not just be used for a specific case investigation. Again, there are appearance issues in accepting

resources of such significant value from an entity that may be the subject of Department action in another arena. This type of offer also directly impacts the Department's operations and mission. However, the company is also offering a capability that is unparalleled. Given the magnitude of this offer, high-level attention to determine whether this offer may be accepted is warranted.

Index

A

B

C

D

E

F

G

I

J

K

L

M

N

O

Q

R

S

T

U