U.S. Department of Justice
Executive Office for United States Attorneys

PROSECUTING INTELLECTUAL PROPERTY CRIMES

Third Edition

Computer Crime and
Intellectual Property Section
Criminal Division

September 2006

Michael Battle
Director, EOUSA

Michael W. Bailie
Director, OLE

OLE Litigation Series

Ed Hagen
Assistant Director
OLE

James D. Donovan
Assistant Director
OLE

Michael M. DuBose
Deputy Chief for
Intellectual Property
CCIPS
Criminal Division
Managing Editor

PROSECUTING INTELLECTUAL PROPERTY CRIMES

Third Edition

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

The Office of Legal Education intends that this Manual be used by Federal Prosecutors for training and law enforcement purposes.

The contents of this book provide internal suggestions to Department of Justice attorneys. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by any prospective or actual witnesses or parties. *See United States v. Caceres*, 440 U.S. 741 (1979).

Table of Contents

Detailed Listing

Preface and Acknowledgments

This Manual builds on the success of the editions published in 2001 and 1997 by giving much broader and deeper treatment to all subject areas, while also adding several new topics. To say that this publication is simply an "updated version" of the 2001 manual would seriously understate the nature and scope of the changes. The 2006 Manual was restructured to present the material in a more consistent format that is easier to use; all the chapters were rewritten to add broader and more in-depth coverage of all areas; recent changes to the case law, statutes, and sentencing guidelines are addressed; and new chapters were added to address the Digital Millennium Copyright Act, patent law, and victim issues. Throughout, we try to present material in a way that will be of 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. Although it is undeniably a group effort, no one deserves more credit than Senior Counsel Scott Garland. Scott had primary responsibility for the project, wrote portions of various chapters, and assumed chief editing duties. Many other CCIPS attorneys made significant writing and editing contributions as well, including in alphabetical order: Lily Chinn (on detail), Jason Gull, Eric Klumb, Marie-Flore Kouame, Marc Miller, Jay Prabhu, Jason Reichelt, Andrea Sharrin, Corbin Weiss, and John Zacharia. Former CCIPS attorneys whose efforts also contributed include Michael O'Leary and Ken Doroshow. 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: Jennifer Freundlich, Michael Radosh, Douglas Bloom, Myles Roberts, Tara Swaminatha, Meghan McGovern, and Rebecca Bolin.

Finally, we are grateful to Ed Hagen, Nancy Bowman, 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.

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

I.

Intellectual Property—An Introduction

I.A. Why Is Intellectual Property Enforcement Important?

Intellectual property ("IP") is critical to the vitality of today's economy. IP is an engine of growth, accounting for an increasing share of jobs and trade. In 2002, the core copyright industries alone were estimated to account for 6% or more of U.S. GDP, and in 2005 the overall value of the "intellectual capital" of U.S. businesses—including copyrights, trademarks, patents, and related information assets—was estimated to account for a third of the value of U.S. companies, or about $5 trillion. Stephen Siwek, *Copyright Industries in the U.S. Economy: The 2004 Report* 11 (Oct. 2004) (core copyright industries statistic), *available at* http://www.iipa.com/pdf/2004_SIWEK_FULL.pdf; Robert J. Shapiro & Kevin A. Hassett, *The Economic Value of Intellectual Property* 18 (Oct. 2005) (overall value of intellectual property statistic), *available at* http://www.usaforinnovation.org/news/ip_master.pdf.

Intellectual property rights create incentives for entrepreneurs, artists, firms and investors to commit the necessary resources to research, develop and market new technology 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). Therefore, effective protection of intellectual property rights is essential to fostering creativity and to supporting our economic and financial infrastructure.

This is a pivotal time for intellectual property enforcement. Market and technological developments have converged to create an environment in which the distribution of both legitimate and illegitimate goods flourishes as never before. As economic freedom expands to more and more countries, their manufacturers and consumers are increasingly interconnected due to advances in telecommunication networks, integrated financial markets, and global advertising.

This interconnected global economy creates unprecedented business opportunities to market and sell intellectual property worldwide. Geographical borders present no impediment to international distribution channels. Consumers enjoy near-immediate access to almost any product manufactured in the United States or abroad, and they are accustomed to using the international credit card system and online money brokers (such as PayPal) to make payment a virtually seamless process worldwide. If the product can not be immediately downloaded to a home PC, it can be shipped to arrive by next day air.

However, the same technology that benefits rights-holders and consumers also benefits IP thieves seeking to make a fast, low-risk buck. Total global losses to United States companies from copyright piracy alone in 2005 were estimated to be $30-$35 billion, not counting significant losses due to Internet piracy, for which meaningful estimates were not yet available. *See International Intellectual Property Alliance Submission to the U.S. Trade Representative for the 2006 Special 301 Report on Global Copyright Protection and Enforcement*, at 21 (Feb. 13, 2006), *available at* http://www.iipa.com/pdf/2006SPEC301COVERLETTERwLTRHD.pdf.

Trafficking in counterfeit merchandise presents economic consequences no less severe. It has been estimated that between 5% and 7% of world trade is in counterfeit goods, which is equivalent to approximately $512 billion in global lost sales. U.S. Chamber of Commerce, *What Are Piracy and Counterfeiting Costing the American Economy?* 2 (2005), *available at* http://www.uschamber.com/ncf/initiatives/counterfeiting.htm (following links re "Scope of the Problem"). Counterfeit products are not limited to bootleg DVDs or fake "designer" purses; they include prescription drugs, automobile and airline parts, food products, and insecticides. *See* Stop Counterfeiting in Manufactured

Goods Act, Pub. L. No. 109-181 § 1(a)(2) ("Findings"), 120 Stat. 285, 285 (2006). As a result, the trade in counterfeit merchandise threatens the health and safety of millions of Americans and costs manufacturers billions of dollars each year.

Whether sold via the Internet or at sidewalk stands on New York's famous Canal Street, the harm to the U.S. economy from IP theft is substantial. Total losses suffered by U.S. industries due to their products being counterfeited is estimated at between $200 and $250 billion per year, costing 750,000 American jobs. U.S. Chamber of Commerce, *What Are Piracy and Counterfeiting Costing the American Economy?* 2 (2005). Strong enforcement, both civil and criminal, is therefore essential to fostering creativity and protecting our economic security.

I.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 intellectual property in four distinct areas: copyright, trademark, patent, and trade secrets.

I.B.1. Copyright

The law of copyright is designed to foster the production of creative works and the free flow of ideas by providing legal protection for creative expression. Copyright provides protection against the infringement of certain 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). These exclusive rights include the rights of reproduction, public distribution, public performance, public display, and preparation of derivative works. 17 U.S.C. § 106. Legal protection exists as soon as the work is expressed in tangible form. Copyright law protects the physical expression of an idea, but not the idea itself.

Although civil law protects all the copyright owner's exclusive rights, criminal law primarily focuses on the rights of distribution and reproduction. *See* 17 U.S.C. § 506(a) and 18 U.S.C. § 2319. Those convicted of criminal copyright infringement face up to five years' imprisonment and a $250,000 fine. *Id.*

I.B.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 like protection.

Legal protections for trademarks and service marks not only help protect the goodwill and reputation of mark-owners, but also promote fair competition and the integrity of markets, and 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 March 2006 the criminal trademark statute was amended to also prohibit trafficking in labels or packaging bearing a counterfeit mark, even when the label or packaging is unattached to the underlying good. Individuals convicted of § 2320 offenses face up to 10 years' imprisonment and a $2,000,000 fine.

I.B.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.

I.B.4. Trade Secrets

A trade secret is any secret formula, pattern, device or compilation of information used in a business that has some independent economic value and which is used to obtain an advantage over competitors who do not know or use it. *See* 18 U.S.C. § 1839(3). One of the most famous trade secrets is the formula for manufacturing Coca-Cola. Coca-Cola was accorded trade secret protection in 1920 because the recipe had been continuously maintained as a trade secret since the company's founding in 1892, and it apparently exists to this day. *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).

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 loses its legal protection.

The theft of trade secrets is punishable by up to fifteen years' imprisonment and a $500,000 fine if done to benefit a foreign government or agent, 18 U.S.C. § 1831, and up to ten years' imprisonment and a $250,000 fine in other cases.

I.C. Why Criminal Enforcement?

Although civil remedies may help compensate victimized intellectual property rights-holders, criminal sanctions are often warranted to punish and deter the most egregious violators: repeat and large-scale offenders,

organized crime groups, and those whose criminal conduct threatens public health and safety. Indeed, because many violations of intellectual property rights involve no loss of tangible property and, for infringement crimes, do not even require direct contact with the rights-holder, the intellectual property owner often does not know that it is a victim until an infringer's activities are investigated and prosecuted.

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 intellectual property prosecutors who investigate, prosecute, and coordinate national and international cases of intellectual property theft. This group of specialists helps develop and execute the Department's overall intellectual property 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 intellectual property offenses specifically—falls to the 94 U.S. Attorneys' Offices across the United States and its territories, the Justice Department has designated at least one, and oftentimes more, 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 intellectual property and computer crime who serve as subject-matter experts within their districts. As of this writing, there are approximately 230 CHIP prosecutors designated to handle both computer crime and intellectual property 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 intellectual property and cyber-crime, or where such crimes have the highest economic impact. These specialized squads focus on prosecuting intellectual property offenses such as trademark violations, copyright infringement, and thefts 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 regarding high-tech investigations, and they work closely with victims of intellectual property theft and cyber-crime on prevention efforts. There are currently 25 CHIP Units

consisting of approximately 80 Assistant U.S. Attorneys, in addition to the approximately 150 CHIP prosecutors in the remaining districts and Justice Department divisions.

The combined prosecution efforts of the CHIP network, CHIP Units, and CCIPS create a formidable three-front enforcement attack against intellectual property thieves and counterfeiters. These enforcement efforts will be even more necessary in the future, as advancing technology and changing economies continue to present new challenges.

I.

Intellectual Property—An Introduction

I.A. Why Is Intellectual Property Enforcement Important?

Intellectual property ("IP") is critical to the vitality of today's economy. IP is an engine of growth, accounting for an increasing share of jobs and trade. In 2002, the core copyright industries alone were estimated to account for 6% or more of U.S. GDP, and in 2005 the overall value of the "intellectual capital" of U.S. businesses—including copyrights, trademarks, patents, and related information assets—was estimated to account for a third of the value of U.S. companies, or about $5 trillion. Stephen Siwek, *Copyright Industries in the U.S. Economy: The 2004 Report* 11 (Oct. 2004) (core copyright industries statistic), *available at* http://www.iipa.com/pdf/2004_SIWEK_FULL.pdf; Robert J. Shapiro & Kevin A. Hassett, *The Economic Value of Intellectual Property* 18 (Oct. 2005) (overall value of intellectual property statistic), *available at* http://www.usaforinnovation.org/news/ip_master.pdf.

Intellectual property rights create incentives for entrepreneurs, artists, firms and investors to commit the necessary resources to research, develop and market new technology 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). Therefore, effective protection of intellectual property rights is essential to fostering creativity and to supporting our economic and financial infrastructure.

This is a pivotal time for intellectual property enforcement. Market and technological developments have converged to create an environment in which the distribution of both legitimate and illegitimate goods flourishes as never before. As economic freedom expands to more and more countries, their manufacturers and consumers are increasingly interconnected due to advances in telecommunication networks, integrated financial markets, and global advertising.

This interconnected global economy creates unprecedented business opportunities to market and sell intellectual property worldwide. Geographical borders present no impediment to international distribution channels. Consumers enjoy near-immediate access to almost any product manufactured in the United States or abroad, and they are accustomed to using the international credit card system and online money brokers (such as PayPal) to make payment a virtually seamless process worldwide. If the product can not be immediately downloaded to a home PC, it can be shipped to arrive by next day air.

However, the same technology that benefits rights-holders and consumers also benefits IP thieves seeking to make a fast, low-risk buck. Total global losses to United States companies from copyright piracy alone in 2005 were estimated to be $30-$35 billion, not counting significant losses due to Internet piracy, for which meaningful estimates were not yet available. *See International Intellectual Property Alliance Submission to the U.S. Trade Representative for the 2006 Special 301 Report on Global Copyright Protection and Enforcement*, at 21 (Feb. 13, 2006), *available at* http://www.iipa.com/pdf/2006SPEC301COVERLETTERwLTRHD.pdf.

Trafficking in counterfeit merchandise presents economic consequences no less severe. It has been estimated that between 5% and 7% of world trade is in counterfeit goods, which is equivalent to approximately $512 billion in global lost sales. U.S. Chamber of Commerce, *What Are Piracy and Counterfeiting Costing the American Economy?* 2 (2005), *available at* http://www.uschamber.com/ncf/initiatives/counterfeiting.htm (following links re "Scope of the Problem"). Counterfeit products are not limited to bootleg DVDs or fake "designer" purses; they include prescription drugs, automobile and airline parts, food products, and insecticides. *See* Stop Counterfeiting in Manufactured

Goods Act, Pub. L. No. 109-181 § 1(a)(2) ("Findings"), 120 Stat. 285, 285 (2006). As a result, the trade in counterfeit merchandise threatens the health and safety of millions of Americans and costs manufacturers billions of dollars each year.

Whether sold via the Internet or at sidewalk stands on New York's famous Canal Street, the harm to the U.S. economy from IP theft is substantial. Total losses suffered by U.S. industries due to their products being counterfeited is estimated at between $200 and $250 billion per year, costing 750,000 American jobs. U.S. Chamber of Commerce, *What Are Piracy and Counterfeiting Costing the American Economy?* 2 (2005). Strong enforcement, both civil and criminal, is therefore essential to fostering creativity and protecting our economic security.

I.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 intellectual property in four distinct areas: copyright, trademark, patent, and trade secrets.

I.B.1. Copyright

The law of copyright is designed to foster the production of creative works and the free flow of ideas by providing legal protection for creative expression. Copyright provides protection against the infringement of certain 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). These exclusive rights include the rights of reproduction, public distribution, public performance, public display, and preparation of derivative works. 17 U.S.C. § 106. Legal protection exists as soon as the work is expressed in tangible form. Copyright law protects the physical expression of an idea, but not the idea itself.

Although civil law protects all the copyright owner's exclusive rights, criminal law primarily focuses on the rights of distribution and reproduction. *See* 17 U.S.C. § 506(a) and 18 U.S.C. § 2319. Those convicted of criminal copyright infringement face up to five years' imprisonment and a $250,000 fine. *Id.*

I.B.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 like protection.

Legal protections for trademarks and service marks not only help protect the goodwill and reputation of mark-owners, but also promote fair competition and the integrity of markets, and 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 March 2006 the criminal trademark statute was amended to also prohibit trafficking in labels or packaging bearing a counterfeit mark, even when the label or packaging is unattached to the underlying good. Individuals convicted of § 2320 offenses face up to 10 years' imprisonment and a $2,000,000 fine.

I.B.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.

I.B.4. Trade Secrets

A trade secret is any secret formula, pattern, device or compilation of information used in a business that has some independent economic value and which is used to obtain an advantage over competitors who do not know or use it. *See* 18 U.S.C. § 1839(3). One of the most famous trade secrets is the formula for manufacturing Coca-Cola. Coca-Cola was accorded trade secret protection in 1920 because the recipe had been continuously maintained as a trade secret since the company's founding in 1892, and it apparently exists to this day. *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).

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 loses its legal protection.

The theft of trade secrets is punishable by up to fifteen years' imprisonment and a $500,000 fine if done to benefit a foreign government or agent, 18 U.S.C. § 1831, and up to ten years' imprisonment and a $250,000 fine in other cases.

I.C. Why Criminal Enforcement?

Although civil remedies may help compensate victimized intellectual property rights-holders, criminal sanctions are often warranted to punish and deter the most egregious violators: repeat and large-scale offenders,

organized crime groups, and those whose criminal conduct threatens public health and safety. Indeed, because many violations of intellectual property rights involve no loss of tangible property and, for infringement crimes, do not even require direct contact with the rights-holder, the intellectual property owner often does not know that it is a victim until an infringer's activities are investigated and prosecuted.

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 intellectual property prosecutors who investigate, prosecute, and coordinate national and international cases of intellectual property theft. This group of specialists helps develop and execute the Department's overall intellectual property 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 intellectual property offenses specifically—falls to the 94 U.S. Attorneys' Offices across the United States and its territories, the Justice Department has designated at least one, and oftentimes more, 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 intellectual property and computer crime who serve as subject-matter experts within their districts. As of this writing, there are approximately 230 CHIP prosecutors designated to handle both computer crime and intellectual property 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 intellectual property and cyber-crime, or where such crimes have the highest economic impact. These specialized squads focus on prosecuting intellectual property offenses such as trademark violations, copyright infringement, and thefts 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 regarding high-tech investigations, and they work closely with victims of intellectual property theft and cyber-crime on prevention efforts. There are currently 25 CHIP Units

consisting of approximately 80 Assistant U.S. Attorneys, in addition to the approximately 150 CHIP prosecutors in the remaining districts and Justice Department divisions.

The combined prosecution efforts of the CHIP network, CHIP Units, and CCIPS create a formidable three-front enforcement attack against intellectual property thieves and counterfeiters. These enforcement efforts will be even more necessary in the future, as advancing technology and changing economies continue to present new challenges.

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 punishment. Felony penalties attach when the violation consists of the reproduction or distribution of at least ten copies that are valued together at more than $2,500, or, under amendments enacted in 2005, when the violation involves distribution of a work being prepared for commercial distribution 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. Finally,

this chapter 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* (2005). Other major treatises and articles that may be instructive include William F. Patry, *Copyright Law and Practice* (1994 & Supps. 1995-2000); *Patry on Copyright* (West Publishing, forthcoming 2006); Sylvia Albert *et al.*, *Intellectual Property Crimes*, 42 Am. Crim. L. Rev. 631 (2005); Michael Coblenz, *Intellectual Property Crimes*, 9 Alb. L.J. Sci. & Tech. 235 (1999).

II.A. Overview

II.A.1. What Copyright Law Protects

Copyright law has two goals: to protect the rights of authors, and, thereby, to foster development of more creative works for the benefit of the public. The Constitution, in granting Congress the power to enact intellectual property laws, describes both these goals and the means to achieve it: "To 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 protecting works and incentives for creators of works, on the one hand, and disseminating knowledge and information to the public, on the other, is a constant theme throughout the history of copyright law. *See Twentieth Century Music Corp. v. Aiken*, 422 U.S. 151, 156 (1975).

The creator of an original work of expression, fixed in a tangible medium, is granted for a limited time a copyright, which is the exclusive right to copy, distribute, and make certain other uses of the work. Copyright law protects all "*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." 17 U.S.C. § 102(a) (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 II.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 II.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 in connection with goods or services. They are discussed in Chapter III of this Manual. Trademarks need not be original or creative. Moreover, many trademarks consist of short single words or short phrases that are ineligible for copyright protection. See Section II.B.1.a.ii. of this Chapter. Despite the differences between copyrights and trademarks, some items may be both copyrighted and trademarked, such as the image of Disney's Mickey Mouse.

II.A.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 called the "Copyright Act," and the penalties for criminal infringement are set forth in 18 U.S.C. § 2319.

A number of important copyright provisions that were originally devised by courts, such as the doctrines of fair use and first sale, are now codified in Title 17. *E.g.,* 17 U.S.C. §§ 107, 109. And courts often interpret copyright law in light of new events and technological developments, which in turn creates 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. __, 125 S. Ct. 2764 (2005); *Sony*, 464 U.S. 417.

II.A.3. Relevance of Civil Cases to Criminal Prosecutions

In applying the criminal copyright statutes, civil precedents are often helpful. 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. *See United States v. Wise*, 550 F.2d 1180, 1189 n.14 (9th Cir. 1977) (noting "general principle in copyright law of looking to civil authority for guidance in criminal cases"); *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.

But what makes a good civil case does not necessarily make a good criminal case. Civil and criminal copyright law sometimes differ sharply. For example, a defendant can be civilly liable for copyright infringement as a matter of strict liability, with no intent to copy. *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 II.B.2. of this Chapter.

II.A.4. Federal Preemption

In addition to being primarily statutory, copyright law is also 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 1972.

Consequently, pre-1972 sound recordings may still be protected by state copyrights until 2067. *See La Cienega Music Co. v. ZZ Top*, 53 F.3d 950 (9th Cir. 1995); 17 U.S.C. § 301(c).

II.A.5. When Copyright Protection Begins and Ends

A work is protected by copyright law from the moment it is created, even if it is not registered. *See* 17 U.S.C. §§ 101-102(a), 408(a). Although registration with the Register of Copyrights is not a prerequisite to copyright *protection*, it generally is a prerequisite to civil *enforcement* and to some *remedies*. Registration is generally a prerequisite to a copyright holder's civil suit for infringement. *See* 17 U.S.C. § 411. If the work was registered only after infringement, the plaintiff may still collect actual damages for infringement committed prior to registration, but generally cannot collect statutory damages or attorneys' fees. *See* 17 U.S.C. § 412. The Department's position that registration is not a prerequisite to criminal enforcement, including CCIPS's recommendation that prosecutors obtain registration certificates before trial, is discussed in Section II.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. § 302(b). Works made for hire (e.g., 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 pre-1978 works are protected for 95 years from the date that copyright was first secured (generally their date of publication). 17 U.S.C. § 304.

II.A.6. The Rights Protected by Copyright

Copyrighted law grants copyright holders 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).

The exclusive rights set forth in 17 U.S.C. § 106 are subject to a number of exceptions and limitations in §§ 107-122, such as the right to make limited or "fair use" of a work, to resell one's personal copy of a work, and to reproduce computer software that one owns 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 is infringement. 17 U.S.C. § 501. But not every unlicensed use constitutes an infringement. "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 ....").

II.A.7. When Infringement is Criminal

Not every infringement is a criminal offense. Criminal copyright penalties have always 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 infringement is particularly serious, the infringer knows the infringement is wrong, or the type of case renders civil enforcement by individual copyright owners especially difficult.

Copyright infringement is a crime if the defendant acted *willfully* and either (1) for commercial advantage or private financial gain, (2) by reproducing or distributing 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). Copyright infringement is a felony only if the infringement involved reproduction or distribution of at least 10 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.

II.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) (formerly § 506(a)(1), before the Family Entertainment and Copyright Act of 2005, Pub. L. No. 109-9 § 103, 119 Stat 218, 220-21 (Apr. 27, 2005) amendments)

2. Willful infringement not for profit, but with "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) (formerly § 506(a)(2) before the Apr. 27, 2005 amendments)

3. Pre-release piracy, i.e., 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) (newly enacted with the Apr. 27, 2005 amendments)

The common factors are that (1) there must be a 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," but other courts hold first sale to be an affirmative defense. See Section II.C.4. of this Chapter.

Determining the elements to prove a felony (versus a misdemeanor) is slightly more involved. For-profit infringement, § 506(a)(1)(A), is a five-year felony if:

- The defendant infringed by means of "the reproduction or distribution, including by electronic means," AND
- "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).
- Otherwise—if the offense violated rights other than reproduction or distribution or the offense did not satisfy the monetary or

numerical thresholds—it is a misdemeanor. 18 U.S.C. § 2319(b)(3).

Non-profit infringement, § 506(a)(1)(B), is a three-year felony if

- the defendant infringed by means 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." 18 U.S.C. § 2319(c)(1).
- Otherwise—if the offense did not satisfy the monetary and numerical thresholds—it is a misdemeanor. 18 U.S.C. § 2319(c)(3).

Pre-release infringement over a publicly-accessible computer network, 17 U.S.C. § 506(a)(1)(C), is always a felony, but the penalties increase if it is done for commercial advantage or private financial gain. 18 U.S.C. § 2319(d)(1),(2).

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

1. A copyright exists (see Section II.B.1. of this Chapter)
2. The defendant acted willfully (Section II.B.2.)
3. It was infringed by the defendant by reproduction or distribution of the copyrighted work, or (for violations of 17 U.S.C. § 506(a)(1)(C)), by distribution (Section II.B.3.a.)
4. The infringement consisted of either of the following:

   (a) the defendant infringed 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 II.B.3.b.); OR

   (b) the defendant infringed by

      (i) the distribution

      (ii) by making available on a computer network accessible to members of the public

      (iii) of a "work being prepared for commercial distribution"

      (iv) the defendant knew or should have known the work was being prepared for commercial distribution (Section II.B.3.c.)

Repeat felonies garner increased 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); Family Entertainment and Copyright Act of 2005 (FECA), Pub. L. No. 109-9 § 103, 119 Stat. 218, 220-21 (2005). 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.

II.B.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.

II.B.1.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).

II.B.1.a.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 PC'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 v. Rural Telephone Co.*, 499 U.S. 340, 345-46 (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 rather than original. *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.

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

II.B.1.a.ii. Short Phrases Are Not Copyrightable

Short single words, short phrases, and familiar symbols and designs 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.

II.B.1.a.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 (1991); *Whelan Assoc. v. Jaslow Dental Lab.*, 797 F.2d 1222 (3d Cir. 1986). Novel ideas, methods, and processes may enjoy protection under patent or trade secret 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, which 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.

II.B.1.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 now protect a copyrightable work regardless of whether these formalities have been observed. *See La Resolana Architects, PA v. Clay Realtors Angel Fire*, 416 F.3d 1195, 1198-1205 (10th Cir. 2005). 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 and that the application is proper. *See* 17 U.S.C. § 408(a). That decision to register and the certificate of registration can, however, have legal significance at trial. See Sections II.B.1.d.-e. of this Chapter.

II.B.1.c. New Procedure for "Preregistration"

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); *see also* Copyright Office Preregistration web page, available at http://www.copyright.gov/prereg/. 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. *See* 37 C.F.R. § 202.16. These include movies, musical compositions and sound recordings, computer software and video games, literary works, and "advertising and marketing photographs." *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 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 allows an "action for infringement" to be "instituted" under 17 U.S.C. § 411(a), preregistration, unlike registration, involves only a cursory review by the Copyright Office and consequently preregistration 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 II.B.1.d.-e. of this Chapter.

II.B.1.d. Whether Registration or Preregistration is Required to Prosecute

Section 411 of Title 17 provides that "no action for infringement of the copyright of any United States work shall be instituted until preregistration or registration of the copyright claim has been made in accordance with this title." Because either registration or the "preregistration" process satisfies § 411(a), the term "registration" is used below to refer to both registration and preregistration, except as otherwise noted. The term "pre-registration," including a hyphen, is used to refer to events occurring before registration. Also, § 411 applies only to "United States works," meaning works first published domestically, or works created by U.S. nationals or "habitual residents." *See* 17 U.S.C. §§ 101, 411(a). Thus, registration is not required for civil or criminal cases involving *foreign* works.

The Department contends that the registration/preregistration requirement in § 411 applies only to civil lawsuits, not criminal prosecutions. Section 411 refers only to "actions," a term used elsewhere in the Copyright Act to refer to civil actions, not criminal prosecutions. *See*, *e.g.*, 17 U.S.C. § 507 (using the term "civil action" in contrast to the term "criminal proceedings") and does not explicitly refer to criminal prosecutions. *Cf. United States v. Cleveland*, 281 F. 249, 253 (S.D. Ala. 1922) (holding statutory provision governing "action" not applicable to criminal case because "action" is not ordinarily used to describe criminal prosecution). *But see United States v. Backer*, 134 F.2d 533, 535-36 (2d Cir. 1943) (interpreting substantially identical language in the 1909 Copyright Act to require registration as a precondition to any action for infringement, whether civil or criminal because "action" includes both criminal and civil actions in other contexts); 4 *Nimmer on Copyright* § 15.01[A][2](citing *Backer*); *see also Mason v. United States*, 1 F.2d 279

(7th Cir. 1924) (non-copyright case); *Singleton v. United States*, 290 F. 130 (4th Cir. 1923) (non-copyright case).

The criminal copyright provisions are silent on the issue of registration. Section 507 of Title 17, which sets forth the statutes of limitation for both criminal and civil cases, is entitled "Limitations on Actions," although § 507(a) refers to "Criminal Proceedings," not "actions."

The Department's position is supported by legislative history and dicta from the Supreme Court. Although the Copyright Act's legislative history is largely silent on the question, the Senate Judiciary Committee observed in 1988 that "registration is *not* a statutory precondition for criminal enforcement of copyright." S. Rep. No. 100-352 (1988), *reprinted in* 1988 U.S.C.C.A.N. 3706, 3743 (emphasis added). Although this isolated legislative statement came long after the registration requirement was first imposed, the legislative history appears to contain no other statements that are directly contrary. Instead, other legislative statements are at best inconclusive. *See, e.g.*, 151 Cong. Rec. S450-01, 494 (daily ed. Jan. 25, 2005) (statement of Sen. Hatch) (stating that the Family Entertainment and Copyright Act "will create a pre-registration system that will permit criminal penalties and statutory-damage awards [and] also provide a tool for law enforcement officials.") Moreover, that registration is not required for criminal prosecution seems to be the position of at least some past members of the Supreme Court. *See Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 493 n.44 (1984) (Blackmun, J., dissenting on other grounds; Powell, J., Marshall, J., and Rehnquist, J. joining).

The Department's position is also supported by public policy. Admittedly, requiring registration before a civil suit encourages authors to register their works. But that incentive is attenuated in criminal cases because prosecutions are brought by the government, which has no power to register works on behalf of authors. *See* 17 U.S.C. §§ 106, 408. Moreover, criminal copyright prosecutions protect the public interest in preventing infringement. And infringement of an unregistered copyrighted work is infringement nonetheless. *See* 17 U.S.C. § 408(a) ("[R]egistration is not a condition of copyright protection."); *id.* § 501 ("Anyone who violates any of the exclusive rights of the copyright owner ... is an infringer of copyright"); *id.* § 506(a)(1) ("*Any person* who willfully infringes a copyright shall be punished ....") (emphasis added). Making registration a prerequisite to criminal prosecution could impede criminal prosecution for the public benefit due to a victim's delay or neglect in completing a ministerial task intended primarily to promote administrative efficiency.

Cf. Nadel & Sons Toy Corp. v. William Shaland Corp., 657 F. Supp. 133, 136 (S.D.N.Y. 1987) ("Registration of a copyright is essentially ministerial in nature ....") (citation omitted); Douglas Y'Barbo, *On Section 411 of the Copyright Code and Determining the Proper Scope of a Copyright Registration*, 34 San Diego L. Rev. 343, 353 (1997) ("The purpose of section 411(a) is essentially to facilitate judicial resolution of the ownership issue ....").

As a practical matter, however, the Department generally recommends that prosecutors introduce certificates of registration at trial. Certificates of registration are the simplest way to prove a copyright's validity and ownership. Even assuming registration is not required, without it prosecutors will have to prove these elements "from scratch" through testimony and other evidence. See Section II.B.1.e. of this Chapter. Prosecutors should therefore ensure, to the extent possible, 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.html.

This is not to say, however, that copyright registrations are needed earlier than trial. The government can obtain search warrants, grand jury subpoenas, and even indictments before it has certificates of registration in hand, if only because search warrants and grand jury proceedings are based on findings of probable cause.

Although a lack of registration (which may be a mere oversight, or a conscious choice to delay registration until a work is ready for publication) should not bar a criminal prosecution, the circumstances surrounding the absence of registration may militate against the choice to prosecute. A copyright-holder's refusal to register his copyright even when necessary for trial may indicate—or be interpreted—as the victim's intent to allow others to copy the work. The Copyright Office's refusal to register a work may indicate a weak claim of copyrightability or ownership.

If a court requires registration as a prerequisite to a criminal prosecution for infringement, a number of other questions arise, which are discussed below.

II.B.1.d.i. Liability for Infringement Committed Prior to Registration

If a court requires registration, one question prosecutors may face is whether criminal charges may be based on infringement committed prior to registration. While Title 17 clearly allows for civil infringement actions (and recovery of damages) based on pre-registration infringement, and nothing in the statute indicates a contrary intent with respect to criminal prosecutions, in the only reported criminal case on point a district court held that a criminal copyright prosecution cannot be based on pre-registration infringement. *See United States v. Gallo*, 599 F. Supp. 241, 245 n.1 (W.D.N.Y. 1984) (holding, however, that "[e]vidence as to activities involving PENGO before the registration date could perhaps be relevant to other matters, but not to show copyright infringement or wrongful distribution of PENGO"). The *Gallo* court assumed that "there can be no infringement" until the work in question has been registered—a conclusion that was almost certainly wrong. *See Montogomery v. Noa,* 168 F.3d 1282, 1288 (11th Cir. 1999) (noting that "after 1977, copyright automatically inheres in the work at the moment it is created without regard to whether it is ever registered"); 17 U.S.C. § 302 (1988) (providing copyright protection at the time the work is created); 17 U.S.C. §§ 411-412 (providing registration as prerequisite to initiation of lawsuit and certain types of damages); 2 *Nimmer on Copyright* § 7.16[A][1]; 4 *Nimmer on Copyright* § 15.01[A][2], at 15-4 & n.24 (characterizing *Gallo* as "erroneously assuming that registration is a condition precedent to obtaining copyright rather than to bringing an infringement action"). Moreover, the *Gallo* court's ruling contrasts sharply with well-settled civil precedents holding that an infringement action may be based on conduct that predates the victim's copyright registration. *See, e.g., Chuck Blore & Don Richman Inc. v. 20/20 Advertising Inc.*, 674 F. Supp. 671 (D. Minn. 1987); 2 *Nimmer on Copyright* § 7.16[B][1][a], at 7-153; *Washingtonian Pub. Co. v. Pearson*, 306 U.S. 30, 39 (1939).

Given the *Gallo*'s court's confusing statement, the lack of other relevant criminal case law, and the general principle of applying civil copyright law in criminal copyright cases, the authorities cited above support the Department's position that even if a court requires registration as a prerequisite to prosecution, defendants can still be held criminally liable for pre-registration acts of infringement.

II.B.1.d.ii. Unpublished or Pre-Release Works

Infringement before registration often involves infringement before lawful publication. *Cf. Salinger v. Random House, Inc.*, 811 F.2d 90 (2d

Cir. 1987) (biographer included plaintiff's unregistered and unpublished letters in biography of plaintiff, after which plaintiff registered letters and sued). A typical case for prosecutors might involve pre-release piracy, where the defendant obtains and distributes on the Internet a copy of a new movie before it has been released in theaters, or a new video game before it has been legitimately distributed to the public. *See*, *e.g.*, *United States v. Gonzalez* (S.D.N.Y. 2004) (criminal conviction for posting advance copy of movie "The Hulk" on the Internet) (press release available at http://www.usdoj.gov/criminal/cybercrime/gonzalezPlea.htm).

Although an unpublished work is protected by copyright, a plaintiff in a civil case may not recover attorneys fees or statutory damages for "any infringement of copyright in an unpublished work commenced before the effective date of its registration." 17 U.S.C. § 412(1). Given that civil penalties are limited in such cases, a criminal defendant might argue that criminal penalties for infringement of an unpublished work before registration should similarly be foreclosed. To date, no court appears to have addressed such an argument.

The preregistration procedure available under the Family Entertainment and Copyright Act was designed to address the piracy of certain types of unpublished works, but unfortunately does not resolve whether registration or preregistration of unpublished works is a prerequisite to criminal prosecution for infringement of such works. Nevertheless, the preregistration procedures provides a relatively quick and simple way for a copyright-holder in an unpublished work to satisfy 17 U.S.C. § 411(a). Therefore, prosecutors handling a case involving infringement of unpublished and unregistered works should consider whether preregistration is an option.

II.B.1.d.iii. Registration of Particular Versions of a Work

Should a court hold that registration is a prerequisite to criminal prosecution, the question might arise whether the registration of one version of a work satisfied § 411 if the infringement involved a different, unregistered edition of the work. For instance, computer software is frequently revised and republished in new versions, some registered, some not. If the victim registered version 1.0 but not version 1.5, can the government still pursue a criminal case for infringement of version 1.5? Or, if the circumstances are reversed and the victim registered version 1.5 but not 1.0, can a case be brought for infringement of version 1.0?

Although there is no reported criminal case law on the issue, civil authority suggests that registering a different version of a work will often satisfy § 411. This is especially true if a later version was registered, but

earlier versions had not, which is sometimes referred to as a "backward-looking" registration. In those cases, courts generally have allowed a case to proceed based on infringement of the earlier (though unregistered) version. *See Murray Hill Publ'ns v. ABC Commc'ns*, 264 F.3d 622, 650 (6th Cir. 2001); *Streetwise Maps v. VanDam, Inc.*, 159 F.3d 739, 747 (2d Cir. 1998).

On the other hand, if an early version had been registered, but subsequent versions were not ("forward-looking" registration), courts have been less consistent about whether to allow claims for infringement of the later, unregistered versions. *Compare Montgomery v. Noga*, 168 F.3d 1282, 1292-93 & n.17 (11th Cir. 1999); *Liu v. Price Waterhouse LLP*, 182 F. Supp. 2d 666, 675 (N.D. Ill. 2001) ("No registration is necessary for a derivative work, so long as the underlying original work is registered"); *Central Point Software, Inc. v. Nugent*, 903 F. Supp. 1057, 1060 & n.5 (E.D. Tex. 1995) (allowing infringement claim where plaintiffs registered copyrights in earlier versions of software and defendants copied subsequent versions derived from registered works); *and Video Pipeline v. Buena Vista Home Entertainment*, 275 F. Supp. 2d 543, 556 (D.N.J. 2003) (holding court had jurisdiction over infringement counterclaim where infringement of unregistered derivative work also infringed element of original, registered work) *with Johnson v. Gordon*, 409 F.3d 12, 20 (1st Cir. 2005) (holding claims based on "new elements" present in later, unregistered, "long version" of song could not proceed); *Well-Made Toy Mfg. Corp. v. Goffa*, 354 F.3d 112 (2d Cir. 2003) (holding registration for earlier, 20" version of doll did not grant jurisdiction for claim of infringement of later, 48" version).

If there is a consistent rule for "forward-looking" registration cases, it appears to be that courts will likely allow an action for infringement of a later, unregistered work that incorporates significant portions of an earlier, registered work if the same entity owns both copyrights and the defendant infringed elements that were present in the old registered version as well as the newer one. *See* 2 *Nimmer on Copyright* § 7.16[B][2]; *see also Montgomery*, 168 F.2d at 1292.

II.B.1.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 also United States v. Taxe*, 540 F.2d 961, 966 (9th Cir. 1976); *United States v. Moore*, 604 F.2d 1228, 1234 (9th Cir. 1979). 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.*, *Autoskill, Inc. v. National Educ. Support Sys., Inc.*, 994 F.2d 1476, 1487 (10th Cir. 1993), after which the prosecutor may rebut with evidence showing that the certificate is genuine, the registration was properly obtained, or otherwise that the copyright is 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); *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/circ6.html. 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 copyrights' validity. *E.g.*, *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 v. Clay Realtors Angel Fire*, 416 F.3d 1195, 1208 (10th Cir. 2005); *see also 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.

II.B.1.f. Copyright Notice

Prosecutors should confirm that the copyright in any work did not lapse for failure to include a copyright notice when the work was first published. The effect of publishing a copyrighted work without a copyright notice depends on whether the work was first published before or after March 1, 1989. 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). Their loss of copyright protection would persist to the present day, and thus preclude criminal prosecution for their infringement today. *See* 2 *Nimmer on Copyright* §§ 7.02[C][1]-[3], at 7-16 to 7-17.

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

II.B.2. The Defendant Acted "Willfully"

II.B.2.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).

A lower standard for "willfulness" was advanced by Representatives Goodlatte and Coble, who introduced and sponsored the bill in the House. They rejected the notion that defendant must be familiar with the copyright code and what constitutes infringement. Rather than require "knowledge" of a legal duty not to infringe, they interpreted willfulness to require only that a defendant have "reckless disregard" for copyrights:

> 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.

143 Cong. Rec. 24,325 (1997).

Aside from clarifying that evidence of infringement, by itself, does not prove willfulness, *see supra*, Congress has 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, *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 advocated by Senator Hatch: the intentional violation of a known legal duty. *See* 4 *Nimmer on Copyright* § 15.01[A][2], at 15-6 to 15-7; *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"); *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).

A minority of courts in criminal copyright cases have apparently applied "willfulness" to set a lower bar for 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; Mary Jane Saunders, *Criminal Copyright Infringement and the Copyright Felony Act*, 71 Denv. U. L. Rev. 671, 688 (1994); Sylvia N. Albert *et al.*, *Intellectual Property Crimes*, 42 Am. Crim. L. Rev. 631, 656-57 (2005).

It is not clear, however, that *Backer* represents a 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. *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 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 at 1138 (citation and internal quotation marks omitted); *see also* 2 Paul Goldstein, *Copyright* § 11.4.1, at 11:51-11:52 (2d ed. Supp. 1999) (stating that the government must "prove that the defendant knew that his acts constituted copyright infringement or, at least, knew that there was a high probability that his acts constituted copyright infringement.").

The majority rule in criminal copyright cases for a higher standard of willfulness is also consistent with civil copyright cases, which likewise hold 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.*, *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). 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). Congress's use of the term "willfulness" in closely proximate sections 504 and 506 of the Copyright Act suggests that the term should be interpreted similarly in both criminal and civil cases.

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 II.B.2.b. of this Chapter.

II.B.2.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 determine 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).
- **Actual notice to the defendant that his own conduct was illegal.** *See 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).
- **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).
- **The defendant's past manufacture and distribution of pirated works.** *See 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 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. 2005).
- **The defendant's frivolous or bad-faith claim of compliance with copyright laws, which demonstrates a 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").

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 supposedly 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 II.F. of this Chapter.

II.B.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 by [17 U.S.C. § 106A], 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), 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"). *See* § 106. For purposes of criminal enforcement, 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 being, for criminal enforcement purposes, the public's right to fair use, 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 II.C. of this Chapter.

Felony penalties apply only to infringement of the reproduction or distribution rights. *See* 17 U.S.C. § 506(a). Specifically, felony penalties apply only if the infringement involved either "reproduction and distribution" of a minimum number and value of works, *see* 17 U.S.C. § 506(a)(1)(A) (numbered § 506(a)(1) before the Apr. 27, 2005 amendments) and 18 U.S.C. § 2319(b)(1); 17 U.S.C. § 506(a)(1)(B) (numbered § 506(a)(2) before the Apr. 27, 2005 amendments) 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) (enacted Apr. 27, 2005), 18 U.S.C. § 2319(d)(1). See Section II.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 II.B.4. of this Chapter.

Criminal prosecutions mainly focus on reproduction and distribution, because these are generally the most serious infringements and they incur the most significant penalties. This is not to say, however, that the Department would not or could not investigate and prosecute copyright misdemeanors for a profit-motivated public performance, public display, or derivative work.

II.B.3.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) (numbered § 506(a)(2) before the Apr. 27, 2005 amendments), 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) (numbered § 506(a)(1) before the Apr. 27, 2005 amendments), 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, 10 for repeat offenders.

There is a slight variation in language between the two provisions that set forth a $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) (enacted Apr. 27, 2005) for distribution over a computer network accessible by the public. See Section II.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, it is not always necessary to show that copies were "stolen" in order to show infringing distribution.

II.B.3.a.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 and movies on DVD. Copying need not be so blatant or literal to qualify as infringement, but criminal cases rarely involve defendants who have copied only a small portion of a copyrighted work. Disputes over whether one song sounds too alike another, 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 deserve 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, or even 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, 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); *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. 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. v. Cash Money Records, Inc.*, 394 F.3d 357, 370 (5th Cir. 2004); *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 assumed without proof (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).

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 it is generally better to compare against the original maintained on file at the Register of Copyrights, 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 II.C. of this Chapter.

II.B.3.a.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, including 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 users from "warez" websites on the Internet. Distribution is not limited to sales, but 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, *reprinted in* 1976 U.S.C.C.A.N. 5659, 5675-76 *and* 17 U.S.C.A. § 106 (West 1997) (historical note)).

- **"To the Public"**

Although often referred to merely as "distribution," the right protected by § 106 is the right to distribute copies or phonorecords of the work "*to the public*." § 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.

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 courts have noted that the two terms are "for all practical purposes synonymous." *Ford Motor Co.*, 930 F.2d at 299; *see also Harper & Row, Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 552 (1985); 2 *Nimmer on Copyright* § 8.11[A], at 8-148 to 8-149. 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." "Distribution" is not limited to sales, but also includes other transfer of ownership such as gifts or barter. *Ford Motor Co.*, 930 F.2d at 299 citing H. Rep. 94-1476, 94th Cong., 2d Sess. 62, *reprinted in* 1976 U.S. Code Cong. & Admin. News 5659, 5675-76).

For cases discussing whether distribution "to the public" in several contexts, such as computer networks and subscription based services, see Section II.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 infringement of the distribution right. Although § 602 specifies that unauthorized importation is "actionable under § 501," it does not mention criminal actions under § 506. In cases involving importation, prosecutors may also 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 Without Transferring Them**

It is unclear whether a defendant who merely makes copyrighted material available to others has infringed the distribution right without any evidence of an actual transfer of infringing works. This question might arise if a defendant on a peer-to-peer file-sharing network made copyrighted 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. If there is no 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?

Several civil cases addressing online infringement state, or at least suggest, that the distribution right is infringed at the point when the defendant makes a file publicly available. *See A&M Records v. Napster*, 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."); *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 material on website 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, 203 (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 that hyperlinks on the defendant's website pointed to infringing audio files). *Id.*

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).

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* , at 93-95 (August 2001). This, however, does little to 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.

Moreover, a number of federal courts have held that no distribution occurs unless and until an infringing copy is actually disseminated. *See Obolensky v. G.P. Putnam's Sons*, 628 F. Supp. 1552, 1555 (S.D.N.Y.) (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) (_____ discussing point). The leading copyright treatise also supports this view. *See* 2 *Nimmer on Copyright* § 8.11[A] at 8-149 ("Infringement of [the right to distribute] requires an actual dissemination of either copies or phonorecords.").

To date, the only case to squarely address "making available" in the context of peer-to-peer networks and the new "making available" offense in 17 U.S.C. § 506(a)(1)(C) 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. § 160(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 *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 II.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 would likely 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 II.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 Gamma Audio & Video v. Ean-Chea*, No. 91-11615-2, 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 v. Labus*, 1990 WL 120642 at *5.

The government need not prove an actual dissemination if the charge is conspiracy to violate the criminal copyright laws by means of distribution. Conspiracy is an inchoate crime, so 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 particular, lawfully-acquired copy or phonorecord of a work to sell or otherwise dispose of that copy. This exception is often referred to as the "first sale" doctrine. So, 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 II.C.4.c. of this Chapter.

II.B.3.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

II.B.3.b.i. Generally

The final element for felony offenses under 17 U.S.C. § 506(a)(1)(A) and (B) (numbered § 506(a)(1),(2) before the Apr. 27, 2005 amendments) 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 II.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.B.3.b.ii. Definition of "Retail Value" in this Context

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.*

Under both the plain meaning of the statutory text and the legislative history of the 1992 Copyright Felony Act, "retail value" in this provision was intended to refer to the retail value of the infringed item, i.e., the authentic item that was infringed, in the market in which it is sold. By contrast, the sentencing guidelines use either the value of the "infringed item" or the "infringing item" 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 VIII.C.1.c.iii. of this Manual.

Determining the retail value of a pre-release work can be challenging because pre-release works have no legitimate retail value. 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 7 (1992) (emphasis added), *reprinted in* 1992 U.S.C.C.A.N. 3569, 3575. 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.*, 1992 U.S.C.C.A.N. at 3574-75 (statement of Sen. Hatch); 138 Cong. Rec. 34,371 (1992). Although the Family Entertainment and Copyright Act ("FECA") created a new felony offense to address piracy of "work[s] being prepared for commercial distribution" when committed online, the Act does not specify how the "retail value" of such works should be determined (and although the new offense at 17 U.S.C. § 506(a)(1)(C) does not require proof of a minimum value, pre-release piracy may still be charged under the other felony copyright provisions in § 506(a)(1)(A),(B), which, in conjunction with 18 U.S.C. § 2319, do).

By way of comparison, the sentencing guidelines now specify that pre-release works—"work[s] being prepared for commercial distribution," in the guideline's parlance—should be valued for sentencing purposes at the anticipated retail value of legitimate works upon legitimate commercial

release. *See* U.S.S.G. § 2B5.3 cmt. n.2(A)(vi) (amended Oct. 24, 2005). However, in pre-release cases the guidelines also provide for a 2-level enhancement. *See id.* § 2B5.3(b)(2) (amended Oct. 24, 2005). See Section VIII.C.1.c.iii. of this Manual.

Calculating a work's retail value can be more complicated when the work has been published in multiple versions—which often occurs with software—especially if the court determines that registration or preregistration is a precondition to criminal prosecution. See Section II.B.1.d. of this Chapter. As noted there, civil actions for infringement are permitted only for registered works. Courts addressing the infringement of an unregistered version of a software program of which earlier versions had been registered, have allowed damages only to the extent that the infringed material consists of material from earlier, registered versions. The theory behind this limitation is that an unauthorized copy of the unregistered version is, in reality, not an infringement of the unregistered version itself, but rather an infringement of the earlier registered version *through* the copying of the unregistered version. *See, e.g.*, *Montgomery v. Noga*, 168 F.3d 1282, 1292 (11th Cir. 1999); *Well-Made Toy Mfg. Corp. v. Goffa Intern. Corp.*, 210 F. Supp. 2d 147, 158 (E.D.N.Y. 2002); 2 *Nimmer on Copyright* § 7.16[B][2].

On the other hand, the Eleventh Circuit in *Montgomery v. Noga* upheld a jury instruction that permitted the jury to calculate the plaintiff's actual damages by considering the market value of the unregistered version:

> Having held that the defendants infringed Montgomery's registered copyright in VPIC 2.9a by placing VPIC 4.3 on FLD discs, ... it follows that the jury properly could consider evidence of the injury that the defendants' infringement caused to the value of subsequent unregistered VPIC versions derived from version 2.9a—such as VPIC 4.3—in order to determine the extent of the injury to the value of Montgomery's registered copyright at the time of infringement.
>
> * * *
>
> Obviously, Montgomery's damages could not adequately be measured solely by reference to the market value of VPIC 2.9a as a stand-alone computer program; this value presumably was quite low at the time of the infringement given that revised versions of the program were then available.

168 F.3d at 1294-95. Although the court reviewed the instruction under the highly deferential "plain error" standard because the defendants had not objected to it at trial, *see id.*, the holding should nevertheless support

the analogous proposition that if the infringed work is an unregistered version of software that had been derived from an earlier registered version, the appropriate measure for purposes of 18 U.S.C. § 2319 should be the value of the unregistered version.

To charge a criminal copyright violation as a felony, the government must also 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 simply charge a value greater than $2,500.

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 II.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

II.B.3.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

Effective April 27, 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, 119 Stat 218, 220-21 (Apr. 27, 2005) (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, *reprinted in* 2005 U.S.C.C.A.N. 220. 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 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 government's need to prove monetary and numeric thresholds for the copies involved if the defendant distributed pre-release works on a computer network.

II.B.3.c.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 II.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, a civil copyright case, stated that "distribution" and "making available on a publicly-accessible 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 II.B.E.A.ii and the following Section of this Chapter.

II.B.3.c.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 II.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).

II.B.3.c.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 the "preregistration" process discussed in Section II.B.1.c. of this Chapter. The preregistration process sets forth a basic framework and directs the Copyright Office to establish specific rules for preregistration of "works being prepared for commercial distribution." *See* Family Entertainment and Copyright Act, Pub. L. No. 109-9 § 104(a) (amending 17 U.S.C. § 408(f)). 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, as of this writing, the Copyright Office's interim rules for preregistration cover not only movies, music, and software, but also literary works and advertising or marketing photographs. *See* 37 C.F.R. § 202.16 (2005). This is broader than the four classes specified by 17 U.S.C. § 506(a)(3). Second, the Copyright Office allows for the preregistration of a work if the work has only been started: for example, for motions 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) (2005). Although these standards may suffice for preregistration, prosecutors should generally exercise caution in situations that concern 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 do not appear to have foreclosed the government's power to prosecute infringement that occurs before preregistration or registration of a work.

II.B.3.c..iv. The Defendant Knew or Should Have Known that the Work Was Intended for Commercial Distribution

A 17 U.S.C. § 506(a)(1)(C) offense requires proof of a lower degree of mens rea as to the defendant's awareness that the work was "being prepared for commercial distribution" than the other elements of the offense, which require proof of "willfulness." Under § 506(a)(1)(C), the government need not demonstrate that a defendant had actual knowledge that the infringed work was a pre-release work, but rather, 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.

II.B.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 the crime or a secondary element that can enhance the defendant's maximum sentence. These issues are covered in Sections II.B. (setting out elements) and VIII.C.1.f. (sentencing factors) of this Manual.

II.B.4.a. History

Before 1997, the government had 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 court noted that the government could not have charged the defendant with criminal copyright infringement because he had operated his Internet site for trading pirated works without a profit motive.

But Congress found this unacceptable. When *LaMacchia* was decided, times had already changed. Now, as then, the Internet allows people to engage in large-scale electronic 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 (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 cause substantial financial harm regardless of their motive. *Id.*

To close what was called the *Lamacchia* "loophole," Congress passed the No Electronic Theft Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997), which, among other things, eliminated the government's requirement to prove "commercial advantage or private financial gain" for a felony conviction. *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 proof of willful infringement above certain monetary and numerical thresholds.

Even though a profit motive is no longer required in all cases, it should nonetheless be charged when possible because it increases the defendant's maximum statutory sentence (by turning a 17 U.S.C. § 506(a)(1)(B) offense into a § 506(a)(1)(A) offense with its higher penalties, or by increasing the sentence for a § 506(a)(1)(C) offense), increases his guideline sentencing range, increases jury appeal, and can help defeat baseless claims of fair use. See Sections II.C.5., II.E.1, and VIII.C.1.f. of this Manual.

II.B.4.b. Legal Standard

Essentially, a defendant acts for commercial advantage and private financial gain if he sought a profit. *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 peer-to-peer file-trading network that required new users to contribute pirated material in order to join. *See, e.g.,* Department of Justice Press Release, *Final Guilty Plea in Operation Digital Gridlock, First Federal Peer-to-Peer Copyright and Piracy*

Crackdown (May 31, 2005), *available at* http://www.usdoj.gov/criminal/cybercrime/tannerPlea.htm.

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 infringing products in a business internally 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 the performance of a copyrighted musical composition in a restaurant or hotel without charge for admission to hear it infringes the exclusive right of the owner of the copyright to perform the work publicly for profit); *A&M Records v. Napster*, 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 using pirated drafting software to keep overhead low, a website that offers free pirated software to generate advertising revenue when down loaders 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 v. Shanley*, 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'n 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 (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, 113 (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.").

II.B.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 copyright exists;
2. It 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) (numbered § 506(a)(1) before the Apr. 27, 2005 amendments); 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) (numbered § 506(a)(2) before the Apr. 27, 2005 amendments); 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.

II.C. Defenses

II.C.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).

II.C.2. Jurisdiction

U.S. 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 Communc'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 U.S. 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 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 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); *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 no reported criminal cases address 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 U.S. Charging conspiracy also gives 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).

For more on the lack of extraterritorial application of U.S. copyright law, see United States Copyright Office, *Project Looking Forward Sketching the Future of Copyright in a Networked World, Final Report,* 1998 WL 34336436, at *132 (1998).

II.C.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).

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

II.C.4.a. Operation of the Doctrine

A common defense to a claim of infringement of the distribution right is the "first sale" doctrine, codified in 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 work he has. 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 II.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 business 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 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 (E.D.N.Y. 1994)); *see also* Lemley, 68 S. Cal. L. Rev. at 1244 n.23.

Although no reported criminal cases to date appear to have addressed this issue, 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., Adobe Systems, Inc. v. 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).

II.C.4.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 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.), *cert. denied* sub nom., *McCullock v. United States*, 469 U.S. 1061 (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.3d 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 (8th Cir. 1983); *United States v. Moore*, 604 F.2d 1288, 1232 (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).

II.C.4.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 United States v. Moore*, 604 F.2d 1228, 1232 (9th Cir. 1979) (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.*, *United States v. Drum*, 733 F.2d 1503, 1507 (11th Cir. 1984) (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.").

II.C.4.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 cases have yet addressed this issue.

II.C.5. Fair Use

The fair use doctrine allows people in certain circumstances to use copyrighted material in ways the copyright owner has not authorized and might even forbid if asked. Fair uses are generally limited uses for useful or beneficial purposes with minimal impact on the market for the work. Codified at 17 U.S.C. § 107, the fair use doctrine allows people to reproduce or otherwise use 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. 1103, 1110 (1990). 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 66 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5680, 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. 94-1476, at 66 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5680. 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), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5679. Although the fair use doctrine has developed primarily in civil cases, those cases have precedential weight in criminal cases too.

The first listed 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. 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 is whether the use is "transformative, "or 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." *Acuff-Rose*, 510 U.S. 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 listed 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.* at 586. "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 e-mail 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.

II.C.5.a. Unpublished Works

A defendant's use of an unpublished copyrighted work may qualify as a fair use. Earlier decisions focused on the fact that a work was unpublished (or not yet published) in finding against fair use. The Supreme Court then held that the unpublished nature of work is a "'key, though not necessarily determinative, factor' tending to negate a defense of fair use." *Harper & Row*, 471 U.S. at 552-54 (quoting S. Rep. No. 94-

473 at 54 (1976)). In 1992, however, 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). In fact, this act's sole purpose was to amend 17 U.S.C. § 107 with this provision. The act's legislative history repeatedly underscores that Congress intended there to be no *per se* rule barring the fair use of unpublished works. H.R. Rep. No. 102-836, at 1 (1992), *reprinted in* 1992 U.S.C.C.A.N. 2553, 2553. 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* H.R. Rep. No. 102-836 (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. 1990)). Congress heeded this testimony and thereafter amended the fair use statute to include the fair use of unpublished works, not limiting it to works of historic value.

II.C.5.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 too. However, fair use has rarely been developed in criminal cases, 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 *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 II.B.2.a. of this Chapter. (As indicated in Section II.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, supra.*

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, at least one court has rejected fair use arguments in a civil case 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).

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.

II.C.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 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 opthamological 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 Section 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 II.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, 753 (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. Palladin 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").

II.D. Special Issues

Most of the special issues in criminal copyright law concerning registration, Internet piracy, and pre-release piracy have been addressed throughout the substantive sections of this chapter. Prosecutors who encounter special issues that are not otherwise addressed in this chapter should contact CCIPS at (202) 514-1026 to suggest them for an update to be published in the electronic edition of this Manual.

II.E. Penalties

II.E.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 infringes a copyright willfully ... shall be punished as provided under section 2319 of title 18, United States Code.").

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). For the crimes that qualify as misdemeanors, see Section II.B.5. of this Chapter.

A first-time felony conviction under 17 U.S.C. § 506(a)(1)(A) (numbered § 506(a)(1) before the April 27, 2005 amendments) 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) (numbered § 506(a)(2) before the April 27, 2005 amendments) 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) (newly enacted on April 27, 2005) 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).

II.E.2. Sentencing Guidelines

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

II.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 the usual 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 or 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 *MGM v. Grokster*, 545 US __, 125 S. Ct. 2764 (2005). Although *Grokster* is 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 II.B.1.a. 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 II.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 on the basis 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. *See Moghadam*, 175 F.3d at 1274-77; *United States v. Martignon*, 346 F. Supp. 2d 413, 430 (S.D.N.Y. 2004); *KISS Catalog, Ltd. v. Passport Int'l Prods., Inc.*, 405 F. Supp. 2d 1169 (C.D. Cal. 2005). The cases have reached different results. In *Moghadam*, the court rejected the defendant's claim that § 2319A was invalid because it regulated performances that were not "writings,"and upheld the constitutionality of § 2319A as a valid exercise of Congress's Commerce Clause power. *See* 175 F.3d at 1282. However, the court also acknowledged without deciding (because the question was not preserved on appeal) that the statute may face "another constitutional problem under the Copyright Clause," which allows Congress to protect works only for "limited times." *Id.* at 1274 n.9, 1281. The *Martignon* court held the statute unconstitutional, concluding that Congress may not exercise its Commerce Clause power to enact a "copyright-like" statute not subject to the constitutional restrictions on copyright laws. *Martignon*, 346 F. Supp. 2d at 422. In *Kiss Catalog*, the district court initially found 17 U.S.C. § 1101 unconstitutional, citing *Martignon,* but on rehearing vacated its decision and upheld the statute, relying on *Moghadam*. *See KISS Catalog v. Passport Int'l Prods.*, 350 F. Supp. 2d 823, 837 (C.D. Cal. 2004); *Kiss Catalog*, 405 F. Supp. 2d at 1172-73.

Various 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, Pub. L. No. 109-9, 119 Stat. 218 (enacted April 27, 2005), created a new 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), *reprinted in* 2005 U.S.C.C.A.N. 220.

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, *reprinted in* 2005 U.S.C.C.A.N. 220, 223.

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, *reprinted in* 2005 U.S.C.C.A.N. 221-22.

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 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 DCMA 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." *Dowling*, 473 U.S. 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 IV.F. 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 Racketeering 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

III.A. Introduction

III.A.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, and 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, 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 regional or other origin, material, mode of manufacture, quality, accuracy, or other characteristics of goods or services, or 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 invest heavily in their brands. One who infringes a mark often misleads consumers, steals businesses' sales, 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, and then discusses the criminal counterfeiting statute and the elements of the crime, common defenses, issues unique to this crime, and related statutory penalties. Forms providing sample indictments and jury instructions are provided in Appendix C.

The criminal counterfeit marks statute, 18 U.S.C. § 2320, was amended effective March 16, 2006, pursuant to 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). Discussion of these amendments is integrated throughout this Chapter,

sometimes—but not always—by means of bracketed text. Prosecutors should consult the text carefully to ensure that they are applying the law in effect at the time of the offense.

In addition to this Chapter, prosecutors may refer to the leading treatise on trademark law, J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* (2005), as well as other helpful law review articles such as Sylvia N. Albert et al., *Intellectual Property Crimes,* 42 Am. Crim. L. Rev. 631 (2005); Louis Altman, *Callmann on Unfair Competition, Trademarks and Monopolies*, 4 Callmann on Unfair Comp., T. & Mono. § 22:53 (2003); Debra D. Peterson, *Criminal Counterfeiting and Component Parts: Closing the Perceived "Label Loophole,"* 30 AIPLA Q.J. 457 (2002); Michael Coblenz, *Intellectual Property Crimes*, 9 Alb. L.J. Sci. & Tech. 235 (1999); 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 services, service marks, and certification marks as well.

III.A.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 (2005). 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:

1. 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. Rep. 109-68, at 8 n.2 ("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. 98-526, at 4-5 (1984), *reprinted in* 1984 U.S.C.C.A.N. at 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*.

2. 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. Rep. 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 *United States v. Hon*, 904 F.2d 803, 806 (2d Cir. 1990) and S. Rep. 98-526, at 4-5, *reprinted in* 1984 U.S.C.C.A.N. at 3630-31); 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 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3627, 3630-31. 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.

3. 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 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 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3627, 3630-31.

4. 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).

III.B. Elements

III.B.1. The Trademark Counterfeiting Crime in General

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

> 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.

The bracketed language was inserted by the Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1(b)(1), 120 Stat. 285, 285 (Mar. 16, 2006), and thus applies only to offenses arising after its enactment.

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.

To establish a criminal offense under 18 U.S.C. § 2320, the government must prove the following elements (presented here with sub-elements for clarity):

1. The defendant intentionally trafficked or attempted to traffic in goods or services [after March 16, 2006: or labels, documentation or packaging for goods or services]
2. The defendant used a counterfeit mark on or in connection with those goods or services [after March 16, 2006: or a counterfeit mark was applied to labels, documentation, or packaging for those goods or services]
    a. The counterfeit mark was not genuine or authentic
    b. The counterfeit mark was identical to or indistinguishable from a genuine mark owned by another
    c. The genuine mark was registered on the principal register in the United States Patent and Trademark Office
    d. The genuine mark had been in use by the mark-holder or its licensee
    e. The counterfeit mark was used "on or in connection with" the defendant's goods or services [after March 16, 2006: 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"]
    f. The counterfeit mark was used "in connection with" the type of goods and services for which the protected mark was registered [after March 16, 2006: or 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"]

g. The counterfeit mark was used in a manner "likely to cause confusion, to cause mistake, or to deceive"

3. The defendant knowingly used the mark and knew that the mark was counterfeit

The bracketed language was inserted or amended by the Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1, 120 Stat. 285, 285-87 (Mar. 16, 2006). The government must also choose an appropriate venue. These elements are discussed in detail below.

III.B.2. Relevance of Civil Trademark Law in Criminal Cases

Before discussing the elements, it is important to note that 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(c), (e)(3), and the discussion in Section III.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. 31,675-77 (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 one defendant's § 2320 conviction by relying not only on the criminal statute's legislative history, but also on two civil Lanham Act cases, noting that the "definition of the term 'counterfeit mark' in the Lanham Act is nearly identical to the definition [of counterfeit mark] under 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(e)(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, 1351-52 (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).

III.B.3. Intentionally Trafficked or Attempted to Traffic in Goods or Services [after March 16, 2006: 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 [after March 16, 2006: 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 to do so. 18 U.S.C. § 2320(a); *see* Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1, 120 Stat. 285, 285-87 (Mar. 16, 2006).

III.B.3.a. Intentionally

The term "intentionally" modifies "traffics or attempts to traffic in goods or services." *Id.*; *see 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).

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).

III.B.3.b. Trafficked or Attempted to Traffic

III.B.3.b.i. General Definition

Before March 16, 2006, "traffic" was defined in 18 U.S.C. § 2320(e)(2) 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 broad, covering all aspects of commercial activity from initial manufacture to distribution and sale, but was not intended to cover purchases for personal use. *See Joint Statement*, 130 Cong. Rec. 31,675 (1984); S. Rep. 98-526 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3627; David J. Goldstone et al., *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 this broad definition arguably regulated 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 III.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. It defines "traffic" as follows:

> (e)(2) the term "traffic" means to transport, transfer, or otherwise dispose of, to another, ~~as consideration for anything of value~~ [for purposes of commercial advantage or private financial gain], or [to] make[, import, export,] ~~or~~ obtain control of[, or possess,] with intent to so transport, transfer, or otherwise dispose of;

for which

> (e)(3) [the term 'financial gain' includes the receipt, or expected receipt, of anything of value].

Pub. L. No. 109-181, § 2, 120 Stat. 285, 288 (2006) (amending 18 U.S.C. § 2320(e)(2), (3) (adding brackets and strikethrough to show amendment from prior law). These issues are discussed below.

III.B.3.b.ii. Consideration vs. Commercial Advantage and Private Financial Gain

Under the prior definition of "traffic," the thing "of value" that a defendant had to receive as consideration 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), with "financial gain" defined as including "the receipt, or expected receipt, *of anything of value*," § 2320(e)(3) (as amended) (emphasis added).

The "consideration" requirement may have been too narrow to capture some types of commercially-motivated counterfeiting conduct: at least one court held that the term 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 § 2320(e)(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 II.B.4. of this Manual. The cases discussed there should be persuasive in counterfeit mark cases arising after the 2006 amendments.

One type of conduct that the term "traffic" does not include, however, is consumers' knowing acquisition of counterfeit items solely for personal use. This was true under the prior version of "traffic." *See Joint Statement*, 130 Cong. Rec. 31,675 (1984). It is also true after the 2006 amendments, given that "commercial advantage and private financial gain" does not include acquiring infringing items for personal use. See Section II.B.4. of this Manual.

III.B.3.b.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(e)(2) ("[T]he 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 [-]") (showing 2006 amendments); *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* them 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.

III.B.3.b.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 prior 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) ("[T]he term 'traffic' means to *transport*, transfer, or otherwise dispose of, to another ...") (emphasis added) (pre-2006 amendments); *United States*

v. DeFreitas, 92 F. Supp. 2d 272, 276-77 (S.D.N.Y. 2000) (holding that importing counterfeit items from China into the United States for sale constituted trafficking under § 2320). The 2006 amendments make it even more clear that the acts of importing and exporting counterfeits violate § 2320.

III.B.3.c. Goods and Services [after March 16, 2006: and Labels, Patches, Stickers, Wrappers, Badges, Emblems, Medallions, Charms, Boxes, Containers, Cans, Cases, Hangtags, Documentation, or Packaging of Any Type or Nature]

What may the defendant not traffic in? Before the March 16, 2006 amendments in the Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1, 120 Stat. 285, 285-88 (2006), the list included only goods or services.

"Goods and services" are defined by neither § 2320 nor the Lanham Act. Section 2320's legislative history, however, provides some guidance regarding the meaning of "goods," given Congress's focus there on the damage done 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 the 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, 995 (Fed. Cir. 1985); *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. If the defendant used a counterfeit mark but did not provide the good or service himself, then he 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). See Section III.B.4.f. of this Chapter.

Dissatisfied with the *Giles* decision, Congress amended § 2320 to 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) (bracketed language inserted by the Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1(b)(1), 120 Stat. 285, 285 (Mar. 16, 2006)); *see* H. Rep. No. 109-68, at 7 ("This modification is intended to overrule the holding in the case *United States v. Giles* ...."). Thus, after March 16, 2006, defendants can 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 III.C.E. and III.D.2.-3. 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. That certificate will indicate whether the mark in question had been registered for goods or for services, and also for what type of good or service. See Section III.B.4.c. of this Chapter.

III.B.4. The Defendant Used a "Counterfeit Mark" On or In Connection With Those Goods or Services [after March 16, 2006: or a Counterfeit Mark Was Applied to Labels, Documentation, or Packaging for Those Goods or Services]

The government must prove that the defendant knowingly used a counterfeit mark on or in connection with goods or services, or, after the 2006 amendments, that a counterfeit mark was applied to the labels, documentation, or packaging. 18 U.S.C. § 2320(a).

III.B.4.a. Definition of Counterfeit Mark Generally: 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(e)(1)(A), (as amended by the Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1(b)(3), 120 Stat. 285, 286-87 (Mar. 16, 2006)) (brackets and strikethrough added to show amendments).

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

Although this definition indicates that what must be counterfeit is the mark itself, not the goods or services [or, after March 16, 2006, the labels, documentation, or packaging], 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. 2006). In *United States v. Petrosian*, 126 F.3d 1232 (9th Cir. 1997), 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. 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 (citations omitted). See also Section III.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(e)(1)(B) also includes designations protected by the Olympic Charter Act. See Section III.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.
- Woodsy the Owl.

See 18 U.S.C. §§ 700-716.

III.B.4.b. The Counterfeit Mark Must Be Identical to or Indistinguishable from a Genuine Mark Owned by Another

Under 18 U.S.C. § 2320(e)(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' operation). If the criminal and civil standards diverge at all—and the legislative history suggests otherwise, notwithstanding a statement to the contrary in *United States v. Guerra*, 293 F.3d 1279, 1288 (11th Cir. 2002)—the criminal standard should be interpreted more narrowly only in cases at the outer margins, *Id.* (citing *Joint Statement*, 130 Cong. Rec. 31,675 (1984) (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 the criminal and civil standards are the same or 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)(b), which by its terms falls short of being counterfeit.

The phrase "substantially indistinguishable from" is intended to prevent a counterfeiter from escaping liability by modifying a protected

trademark in trivial ways; however, it is not intended to cover cases in which the infringement is arguable, less than clear, or merely "reminiscent of" protected trademarks. *Joint Statement*, 130 Cong. Rec. 31, 676 (1984).

> [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.

Guerra, 293 F.3d at 1288 (quoting *Joint Statement*, 130 Cong. Rec. 31,676 (1984)). Thus, the 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. *Id.* 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, S.A. v. Snyder*, 718 F.2d 524, 531-32 (2d Cir. 1983) (noting that these examples might create a likelihood of confusion without being substantially indistinguishable, in case interpreting Customs's power to seize counterfeits), *cited with approval in Joint Statement*, 130 Cong. Rec. at 31,675-76. However, a counterfeiter who sells a look-alike with an altered brand name can still be convicted if his look-alike reproduces other registered trademarks. *See United States v. Yi*, __F.3d__, 2006 WL 2294854, at *1 n.1, *3 n.4 (5th Cir. Aug. 10, 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).

In the end, what constitutes a "substantially indistinguishable" difference "will need to be elaborated on a case-by-case basis by the courts." *Joint Statement*, 130 Cong. Rec. 31,675 (1984).

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); J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* § 19:58 (4th ed. & June 2002 database update) ("'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 (May 13, 2004). 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 with 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.* Instead, the court ruled that introducing registered trademark designs and labels produced by authorized licensees was sufficient. *Id.* 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). In civil cases, courts have also allowed evidence of actual confusion, such as customers who were fooled, and trademark surveys. 3 J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* §§ 23:2.1; :13, :63. Market surveys are often used in civil cases, but can raise evidentiary issues. *See, e.g.,* 5 *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 III.B.4.g. of this Chapter, which discusses how to prove likelihood of confusion.

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 Montres Rolex, S.A.*, 718 F.2d 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 III.B.2. of this Chapter), and the difference between likelihood of confusion and being substantially indistinguishable.

III.B.4.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(e)(1)(A)(ii), unless the case involves the Olympic symbols; see Section III.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 III.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); *Omega S.A. v. Omega Eng'g*, 228 F. Supp. 2d 112, 120 & n.26 (D. Conn. 2002); *Duluth News-Tribune v. Mesabi Publ'g Co.*, 84 F.3d 1093, 1096 n.2 (8th Cir. 1996); *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*, 165 Fed. Appx 584,85-86 (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 FBI agent who testified that the items seized at the defendant's business were identical to items registered as trademarks in the United States Patent Office.

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(e)(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") (pre- and post-2006 amendments). *See also United States v. Sung*, 51 F.3d 92, 93-94 (7th Cir. 1995) (holding that § 2320(e)(1)(A)(ii) imposes on defendants "the duty to inquire about the [registration] status of the mark") (citations omitted).

III.B.4.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(e)(1)(A)(ii) (both pre- and post-2006 amendments), except in cases involving protected Olympic symbols, as discussed in Section III.D.8. of this Chapter.

What "in use" means cannot be found in the statute, its legislative history, or 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).

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.

What will suffice, however, is 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(e)(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"), *aff'd*, 413 F.3d at 1248; *Guerra*, 293 F.3d at 1290-91. 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.

III.B.4.e. Use of the Counterfeit Mark "On or In Connection With" Goods or Services

Before the March 16, 2006 amendments, the government had to prove that the defendant used the counterfeit mark "on or in connection with" goods or services. 18 U.S.C. § 2320(a). After March 16, 2006, the government must similarly prove that the defendant used the counterfeit mark "on or in connection with" goods or services (just as before), or, in the case of labels, documentation, packaging, and the like, that the counterfeit mark was "applied thereto." 18 U.S.C. § 2320(a) (as amended by the Stop Counterfeiting in Manufactured Goods Act, Pub L. No. 109-181, § 1, 120 Stat. 285 (Mar. 16, 2006)). In addition, the government must prove that the counterfeit mark "is applied to or used in connection with the goods or services" or "is applied to or consists of" a label, documentation, packaging, or the like—in which case the label, documentation, or packaging must be "designed, marketed, or otherwise intended to be used *on or in connection with* the goods or services for which the mark is registered." § 2320(e)(1)(A)(iii) (as amended Mar. 16, 2006) (emphasis added). The changes will largely be insignificant, except in cases involving labels, documentation, or packaging.

The new term from the 2006 amendments, "applied to," is presumably synonymous with "on," but was included because § 2320 was expanded to cover things like labels, documentation, and packaging, which can either be applied to goods and services or have a counterfeit mark applied to them.

The 2006 amendments also recognize that the 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 III.B.3.c. of this Chapter.

Presumably, "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, a person who trafficked in labels, documentation, or packaging—unattached to the underlying goods—may have been prosecuted, albeit only under a theory of conspiracy or aiding-and-abetting. See Section III.B.3.c. of this Chapter. The 2006 amendments, however, allow such a defendant to be charged under § 2320 directly, 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(e)(1)(A)(iii) (as amended Mar. 16, 2006).

III.B.4.f. The Counterfeit Mark Must Have Been Used for the Same Type of Goods or Services for Which the Genuine Mark Was Registered

Before the March 16, 2006 amendments, § 2320's definition of a "counterfeit mark" allowed prosecution only if the defendant's mark was "used in connection with trafficking in goods or services [and was] identical with, or substantially indistinguishable from, a mark *registered for those goods and services* on the principal register in the United States Patent and Trademark Office." 18 U.S.C. § 2320(e)(1)(A)(i)-(ii) (emphasis added) (but see Section III.D.8. of this Chapter concerning cases involving Olympic symbols). Congress intended this requirement as 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 goods and services the defendant trafficked in match the 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 goods or services indicated on the registration certificate, and not directly on the underlying goods or services themselves? Before the 2006 amendments, this scenario exposed a loophole in the law. In *United States. v. Giles*, 213 F.3d 1247, 1251 (10th Cir. 2000), the Tenth Circuit reversed a § 2320 conviction because, among other reasons, the victim had registered its trademark for use on purses and handbags, but not for use on patches—which the defendant sold with counterfeit marks for customers to attach to purses and handbags. See the discussion in Section III.B.3.c. of this Chapter, and also compare *Playboy Enters., Inc. v. Universal Tel-A-Talk, Inc.*, No. CIV. A. 96-CV-6961, 1998 WL 288423 (E.D. Pa. June 3, 1998) (holding that Playboy failed to state an actionable civil claim because its marks had not been registered for use on Internet Web sites). Such conduct could have been prosecuted under § 2320 in certain circumstances—perhaps on the theory that the marks were used "in connection with" the goods and services for which the mark was registered, or under conspiracy or aiding-and-abetting charges (see Section III.B.4.e. of this Chapter)—but a potential loophole complicated such prosecutions.

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* Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1, 120 Stat. 285 (Mar. 16, 2006). See also Section III.B.3.c. of this Chapter. In doing so, Congress did not relax the requirement of matching the defendant's goods and services to those 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(e)(1)(A)(iii) (as amended by the Stop Counterfeiting in Manufactured Goods Act, Pub L. No. 109-181, § 1, 120 Stat. 285, 287 (Mar. 16, 2006)). Note that the 2006 amendments moved this requirement from § 2320(e)(1)(A)(ii) to (e)(1)(A)(iii). *Id.*

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 III.B.4.c. of this Chapter.

III.B.4.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(e)(1)(A)(iii) (pre-2006 amendments); § 2320(e)(1)(A)(iv) (as amended by the Stop Counterfeiting in Manufactured Goods Act, Pub L. No. 109-181, § 1, 120 Stat. 285, 286-87 (Mar. 16, 2006).) (For the standards in cases involving protected Olympic symbols, see Section III.D.8. of this Chapter.) 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, because the fake goods were priced comparatively low, or because the defendant specifically told the purchaser that the goods were counterfeit. Courts have uniformly rejected these arguments. *See, e.g., United States v. Foote*, 413 F.3d 1240, 1246 (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). For example, in *Foote*, because the defendant "openly advertised that he sold counterfeit merchandise" and "informed each customer that his merchandise was fake," he argued that 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.

The doctrine that supports a finding of confusion in such cases is that 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., Foote,* 413 F.3d at 1245; *Yamin*, 868 F.2d at 133. "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." *Torkington,* 812 F.2d at 1353 (emphasis added) (citations omitted). *See also* S. Rep. No. 98-526 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3627. This doctrine was originally developed by courts in interpreting the identical confusion provision in the Lanham Act. *See* 3 J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* § 23:7 (4th ed. 2005).

Courts adopted the post-sale confusion 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; *see also* H. Rep. 109-68, at 8 n.2 ("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) (legislative history to Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1, 120 Stat. 285 (2006)). Interpreting "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. This is the same reason why the government need not demonstrate that the counterfeit product is of lesser quality than the genuine product. Even if the consumer is not defrauded, the counterfeiter is still trading off another's name without his authorization. See Section III.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.,* 3 J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* §§ 23:2.1, :13, :17, :63. 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).

To determine likelihood of confusion in criminal cases, the Eleventh Circuit has applied a test that was developed in civil cases. *See Torkington*, 812 F.2d at 1354. The relevant factors are:

1. Type of trademark
2. Similarity of design
3. Similarity of product
4. Identity of retail outlets and purchasers
5. Similarity of advertising media used
6. Defendant's intent
7. Actual confusion

Id. No one factor is essential; all seven are weighed in an equitable determination by the fact finder. *Id*. This test was originally developed under civil law to determine whether infringement had occurred when the underlying goods are different. *Hon*, 904 F.2d at 808. But when the goods are "identical and the jury has concluded that the [government] has met the two-pronged *mens rea* standard of section 2320, a requirement that confusion among actual or potential purchasers be shown is unnecessary." *Id. See also Polaroid Corp. v. Polarad Elecs. Corp.*, 287 F.2d 492, 495 (2d Cir. 1961) (test often used in civil cases, unless goods are identical and directly competitive). *See generally* 3 *McCarthy on Trademarks and Unfair Competition* § 23.19 (discussing multi-factor tests for likelihood of confusion). In any event, criminal jury instructions need not set forth

this seven-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." 3 *McCarthy on Trademarks* § 23:41 (4th ed. 2005) (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. *3 McCarthy on Trademarks* § 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* 3 *McCarthy on Trademarks* §§ 23:58-:59. *But see Louis Vuitton Malletier v. Dooney & Bourke, Inc.*, 454 F.3d 108, 112 (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*, __F.3d__, 2006 WL 2294854, at *1 n.1, *3 n.4, 9 & n.14 (5th Cir. Aug. 10, 2006).

III.B.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. After the 2006 amendments, in cases involving counterfeit marks on 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 (Mar. 16, 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, 148 (3d Cir. 2005) (quotations 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*, 2000 WL 1036199, at *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.
- 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. Jewell*, 532 F.2d 697, 699-702 (9th Cir. 1976) (cited in § 2320's legislative history) (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); *United States v. Hamamoto*, No. 99-10019, 2000 WL 1036199, at *1 (9th Cir. July 27, 2000) (bribes to defendant, a customs agent in Guam, to clear airway bills for goods imported from Korea, a primary source of counterfeit goods to Guam); *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); *United States v. Guerra*, 293 F.3d 1279, 1288 (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. 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(e)(1)(A)(ii) imposes on the defendant "the duty to inquire about the status of the mark"); *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*, __F.3d__, 2006 WL 2294854, at *3-*4 (5th Cir. Aug. 10, 2006) (holding that 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).

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 III.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).

III.B.6. Venue

An interesting case involving venue and foreign purchases of counterfeit trademarked goods is *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.*

III.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.

III.C.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(e)(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 (Mar. 16, 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 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. 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." *Joint Statement*, 130 Cong. Rec. 31,676 (1984) (internal quotation marks and citation omitted). Thus, "[i]f a licensee manufactures overruns during the course of the valid license, the marks on those goods will remain noncounterfeit for the 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(e)(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 overrun goods defense does not, however, allow counterfeiters to escape criminal liability by attaching real or overrun labels to counterfeits. As discussed in Section III.B.4.a. of this Chapter (citing 4 J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* § 25:15 (4th ed. 2006) and *United States v. Petrosian*,126 F.3d 1232, 1234 (9th Cir. 1997)), it is standard trademark law—both civilly and criminally—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." § 2320(e)(1)(B) (emphasis added). 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, however, have a few limits. 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." *Id.* at 31,676-77. 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 III.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.), *cert. denied*, 125 S. Ct. 676 (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 First 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.* 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).

III.C.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 III.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(e)(1) declares that such goods are not counterfeit. The burden of proof on this issue, as with overrun goods, is placed on the defendant.

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 III.C.3. of this Chapter.

III.C.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 (Mar. 16, 2006).

The case of *United States v. Hanafy*, 302 F.3d 485 (5th Cir. 2002), established the first half of the rule, that a defendant cannot be prosecuted under 18 U.S.C. § 2320 for repackaging genuine goods with reproduced trademarks if the defendant did so without deceiving or confusing others. 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 III.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.

The case of *United States v. Milstein*, 401 F.3d 53, 62-63 (2d Cir. 2005), confirmed the second half of the rule, that the 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. *Milstein*, 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 *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 wrote *Hanafy* and *Milstein* into the newly-enacted § 2320(f): "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." § 2320(f) (as amended Mar. 16, 2006)). The legislative history confirms that Congress intended to codify *Hanafy*. *See* H. Rep. No. 109-68, at 8 & n.1 (2005). "Because 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." *Id.* at 8.

The newly-enacted language also, however, codifies the rule set in *Milstein* of allowing 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 the above cases concern consumables such as food and drugs, similar issues arise in other industries. *See, e.g.*, United States Attorney's Office, Eastern District of New York, *New York Electronic Crimes Task Force Arrests Two Individuals on Charges of Trafficking in Counterfeit Computer Chips and Software* (June 22, 2000) (computer chips remarked to indicate ability to operate at a higher speed than the manufacturer's rating),*available at* http://www.cybercrime.gov/platinum.htm; *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).

Section 2320(f) 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." § 2320(f) (as amended) (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 Cosmetics Act, 21 U.S.C. §§ 331(a), 333, 343, 352, 362, which punishes trafficking in misbranded food, drugs and cosmetics. See Section III.F. of this Chapter.

III.C.4. Lanham Act Defenses

The Lanham Act's civil defenses have been incorporated as defenses against criminal charges brought under § 2320. "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(c). However, "only those defenses, affirmative defenses, and limitations on relief [in the Lanham Act] that are relevant under the circumstances will be applicable." *Joint Statement*, 130 Cong. Rec. 31,675 (1984). 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. 15 U.S.C. § 1115 (b). 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 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 III.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) (Oct. 6, 2005), the mark-holder's unclean hands are less relevant in a criminal case, where 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*, 26 F.3d 135 (9th Cir. 1994) (unpublished) (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,* 888 F.2d 1387 (4th Cir. 1989) (per curiam) (unpublished) (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).

III.C.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(c) 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).

III.D. Special Issues

III.D.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.) (affirming conviction under § 2320 for irregular garments purchased from factories that manufactured garments to trademark holder's specifications), *cert. denied*, 125 S. Ct. 676 (2004); *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: Subsection 2320(a) and (e) 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 III.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).

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 III.B.4.g. of this Chapter.

III.D.2. Counterfeit Goods with Genuine Trademarks

Although the definition of "counterfeit mark" in § 2320(e) 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 III.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 III.C.3 of this Chapter.

III.D.3. Selling Fakes While Admitting That They Are Fakes

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

III.D.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(e). The defendant's own Acme mark is, in fact, a genuine mark.

III.D.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. 2005).

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. *U.S. 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(e)(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 III.E.3. of this Chapter.

III.D.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.

III.D.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 U.S. 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", and 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 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 under 18 U.S.C. § 371.

If the defendant infringed only one trademark, the defendant can be charged with a single count. However, separate sales of goods bearing the same counterfeit mark 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 18 U.S.C. § 2320(a)) (emphasis in original) (footnote omitted).

The courts have not yet addressed several sentencing 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, *Federal Grand Jury Practice* § 11.29 (2000) ("Duplicitous indictments").
- 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 sneaker wrapped in counterfeit packaging may be charged in one count that covers both the sneaker and packaging, and/or whether charging the sneaker and packaging separately in multiple counts is necessary or permissible, now that § 2320 (as amended Mar. 16, 2006) criminalizes trafficking in counterfeit labels,

documentation, and packaging in addition to counterfeit goods and services.

III.D.8. Olympic Symbols

The definition of "counterfeit mark" in § 2320(e)(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 United States Patent and Trademark Office ("USPTO"). Section 2320(e)(1)(A)'s registration requirements do not apply to cases dealing with criminal trademark infringement of Olympic symbols. *Compare* 18 U.S.C. § 2320(e)(1)(A)(ii) *with* § 2320(e)(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 III.B.4.c. of this Chapter.
- Section 2320(e)(1)(A)(ii)'s use requirement does not apply to cases involving protected Olympic symbols. See also the discussion of use in Section III.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 III.B.4.f. of this Chapter.
- In cases involving protected Olympic symbols, the mark is counterfeit under 18 U.S.C. § 2320(e)(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 III.B.4.g. of this Chapter.

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

III.E. Penalties

III.E.1. Fines

An individual defendant can be fined a maximum of $2,000,000 for a first offense or $5,000,000 for subsequent convictions, or twice the monetary loss or gain. *See* 18 U.S.C. §§ 2320(a) (trademark fines), 3571(b), (d). A corporate defendant can be fined a maximum fine of $5,000,000 for a first offense or $15,000,000 for subsequent convictions, or twice the monetary gain or loss. *See* 18 U.S.C. §§ 2320(a), 3571(c), (d).

III.E.2. Imprisonment

The maximum term of imprisonment is 10 years for a first offense and 20 years for subsequent convictions. A defendant can be fined and/or imprisoned. 18 U.S.C. § 2320(a). 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. 00-20091-01KHV, 2003 WL 22466158, at *2-3 (D. Kan. 2003), *aff'd in part on other grounds*, 413 F.3d 1240 (10th Cir. 2005).

III.E.3. Restitution

Before the 2006 amendments, § 2320 contained no express provision for restitution, but restitution was properly awarded in § 2320 cases 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 2006 amendments made the right to restitution explicit. Newly-amended § 2320(b)(4) now provides that "[w]hen a person is convicted of an offense under this section, the court, pursuant to sections 3556,

3663A, and 3664, shall order the person to pay restitution to the owner of the mark and any other victim of the offense as an offense against property referred to in section 3663A(c)(1)(A)(ii)." 18 U.S.C. § 2320(b)(4) (as amended Mar. 16, 2006). 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. A "victim" is defined in newly-enacted § 2320(b)(5) as having "the meaning given that term in section 3663A(a)(2)," which defines a victim as "a person directly and proximately harmed as a result of the commission of an offense for which restitution may be ordered." There is 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.

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(c) incorporates civil Lanham Act defenses: "[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." *United States v. Sung*, 51 F.3d 92, 94 (7th Cir. 1995). 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 III.D.5. of this Chapter. For cases addressing how to prove notice or the defendant's actual knowledge of registration, see *United Srvs. Auto. Ass'n v. National Car Rental Sys.*, 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*, No. 93 CV 4785, 1998 WL 472505 (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 III.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 ("First, as a form of money damages, restitution *payable to the trademark owner* is proper only if ...") (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.")

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.

III.E.4. Forfeiture

Forfeiture is covered in Chapter VIII of this Manual.

III.E.5. Sentencing Guidelines

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

One of the most difficult issues in sentencing § 2320 offenses concerns how to compute the infringement amount of goods in the defendant's possession to which he had not yet applied a counterfeit mark. If 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), and the prosecution wants to obtain a sentence based on those uncompleted goods, the government must establish with a "reasonable certainty" that the defendant intended to complete and traffic in those goods. *See 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, 94-95 (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 be 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, 862-63 (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).

Nevertheless, when the government can show with reasonable certainty that the defendant would likely have attached the unattached counterfeit labels or packaging to actual product, it should include these items in the infringement amount. Thus, for a defendant caught with counterfeit purses along with generic, no-name purses and labels intended to turn the generic items into counterfeits, the infringement amount may include the number of generic purses or counterfeit labels—whichever is lower. And the infringement amount may also include the excess generic purses (purses for which there was no corresponding counterfeit label) or excess counterfeit labels (labels for which there was no corresponding generic purse) if the evidence of past or potential future sales suggests that the defendant would have acquired the missing elements, completed the manufacture, and attempted to sell these wares.

All these issues are likely to be settled more definitely in the second half of 2006, during the next round of amendments to the Sentencing Guidelines. On March 16, 2006, Congress directed the Sentencing Commission to determine whether the guidelines are "adequate to address situations in which the defendant has been convicted of [a § 2320 offense] and the item in which the defendant trafficked was not an infringing item but rather was intended to facilitate infringement, ... or 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, taking into account cases such as *U.S. v. Sung*, 87 F.3d 194 (7th Cir. 1996)." Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1, 120 Stat. 285, 287 (Mar. 16, 2006). This review of the guidelines will hopefully help resolve how to value uncompleted goods and how to value counterfeit labels, documentation, and packaging.

In the meantime, one principle to bear in mind is that before the Stop Counterfeiting in Manufactured Goods Act was awarded, the appropriate guideline for addressing an uncompleted good to which a counterfeit mark had yet to apply counterfeit labels, documentation, or packaging might have been U.S.S.G. § 2B5.3 in conjunction with U.S.S.G. § 2X1.1 (Conspiracies, Attempts, Solicitations), *see Sung*, 51 F.3d at 94-95, but only because trafficking in counterfeit labels, documentation, and packaging was not a completed crime. Now that the Stop Counterfeiting in Manufactured Goods Act has made trafficking in unattached counterfeit labels, documentation, and packaging a crime on its own, there is some question whether U.S.S.G. § 2X1.1 will apply to such cases.

III.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 III.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 Cosmetics 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 Racketeering Section of the Criminal Division. *See* USAM 9-110.101, 9-110.320.

- **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 designed to protect consumers should contact the Justice Department's Office of Consumer Litigation at (202) 616-0219.

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 Section, which is part of the Consumer Protection Bureau, may be reached at (202) 326-3779. 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, they may be reached by telephone at 1-888-INFO-FDA (1-888-463-6322).

IV.

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

IV.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. 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 be unmasked by a criminal act.

Until 1996, no federal statute explicitly criminalized the theft of commercial trade secrets. Some statutes could punish trade secret theft 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 scheme to use information in violation of a confidential or fiduciary relationship. See Section IV.F. of this Chapter.

In 1996, Congress acted to correct the occasional mismatch between then-existing statutes and commercial trade secret theft by enacting the Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489 (1996) (codified at 18 U.S.C. §§ 1831-1839).

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.* (1985); Roger M. Milgrim, *Milgrim on Trade Secrets* (1994); 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-OCT Fed. Law. 34 (2001); Marc J. Zwillinger & Christian S. Genetski, *Calculating Loss Under the Economic Espionage Act of 1996*, 9 Geo. Mason L. Rev. 323 (2000); Michael Coblenz, *Intellectual Property Crimes*, 9 Alb. L.J. Sci. & Tech. 235 (1999); Sylvia N. Albert et al., *Intellectual Property Crimes*, 42 Am. Crim. L. Rev. 631 (2005); 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).

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

IV.B.1. Overview

The Economic Espionage Act of 1996 ("EEA") criminalizes two types of trade secret misappropriation in Title 18. Section 1831punishes 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 $500,000 or imprisoned not more than 15 years, or both.

18 U.S.C. § 1831(a) (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 or included in a product that is produced for or placed 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) (emphasis added).

Although § 1831 (foreign economic espionage) and § 1832 (commercial economic espionage) define separate offenses, they are nevertheless related. 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 that this information was a trade secret; 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 not only the misappropriation of a trade secret, but also the knowing receipt, purchase, destruction, or possession of a stolen trade secret. *See* 18 U.S.C. §§ 1831(a)(3), 1832(a)(3).

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

If a foreign connection 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 owner of the trade secret would be injured; and (6) the trade secret was related to or was included in a product that was produced or placed in interstate or foreign commerce.

The EEA can be applied to a wide variety of criminal conduct. It criminalizes attempts and conspiracies to violate the EEA and certain extraterritorial conduct. See Sections IV.B.6. and IV.D.3. 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. See Section IV.D. of this Chapter.

For a discussion of the Department of Justice's oversight of EEA prosecutions, see Section IV.D.4.

IV.B.2. Relevance of Civil Cases

The EEA's definition of a trade secret, 18 U.S.C. § 1839(3), is based on the trade secret definition in the Uniform Trade Secrets Act. *See* H.R. Rep. 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.

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

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

IV.B.3.a. The Information Was a Trade Secret

IV.B.3.a.i. Generally

As mentioned in the 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 ..., so that the only way the secret can be unmasked is by [unlawful activity]." *ConFold Pac. v. Polaris Indus.*, 433 F.3d 952, 959 (7th Cir. 2006) (Posner, J.) (citations omitted). Whether particular information is a trade secret is a question of fact. 4 Roger M. Milgrim, *Milgrim on Trade Secrets* § 15.01[1][a][i].

The EEA's definition of a trade secret is very broad. As defined at 18 U.S.C. § 1839, a trade secret includes generally 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:

> (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). As mentioned above, the EEA's definition of a trade secret, 18 U.S.C. § 1839(3), comes from civil law, so cases that address trade secrets outside the EEA should, in most cases, be relevant in EEA prosecutions. See Section IV.B.2. of this Chapter.

Examples of trade secrets include:

- a computer software system used in the lumber industry. *Rivendell Forest Prods., Ltd. v. Georgia-Pacific Corp.*, 28 F.3d 1042, 1046 (10th Cir. 1994).
- measurements, metallurgical specifications, and engineering drawings to produce an aircraft brake assembly. *United States v. Lange*, 312 F.3d 263 (7th Cir. 2002).
- information involving zinc recovery furnaces and the tungsten reclamation process. *Metallurgical Indus. Inc. v. Fourtek, Inc.*, 790 F.2d 1195, 1202 (5th Cir. 1986).
- information concerning pollution control chemicals and related materials. *Apollo Techs. Corp. v. Centrosphere Indus. Corp.*, 805 F. Supp. 1157, 1197 (D.N.J. 1992).
- information regarding contact lens production. *Syntex Ophthalmics, Inc. v. Tsuetaki*, 701 F.2d 677, 684 (7th Cir. 1983).
- pizza recipes. *Magistro v. J. Lou, Inc.*, 703 N.W.2d 887, 890-91 (Neb. 2005).

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 IV.B.6. of this Chapter.

IV.B.3.a.ii. Employee's General Knowledge, Skill, or Abilities Not Covered

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.* 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." *United States v. Martin*, 228 F.3d 1, 11 (1st Cir. 2000) (emphasis in original). "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).

These principles are often cited when the purported trade secret is one the defendant remembered only casually. For example, one court held that a terminated agent cannot be prohibited from using skills that he acquired, or casually remembered information that he acquired, while employed by the principal. *Apollo Techs. Corp. v. Centrosphere Indus. Corp.*, 805 F. Supp. 1157, 1200 (D.N.J. 1992) (quoting Restatement (Second) of Agency § 396 comments b, h). In another case, a court ruled that "[r]emembered information as to specific needs and business habits of particular customers is not confidential." *Tactica Int'l, Inc. v. Atlantic Horizon Int'l, Inc.*, 154 F. Supp. 2d 586, 606 (S.D.N.Y. 2001) (citations omitted). In *Tactica*, the court cited two reasons for finding that remembered information concerning customer preferences was not a trade secret. First, no evidence was offered that the defendants intentionally memorized information, or that they stole it in any other way. *Id.* at 606-07 (citing *Levine v. Bochner*, 517 N.Y.S.2d 270, 271 (N.Y. App. Div. 1987) ("The use of information about an employer's customers which is based on casual memory is not actionable.")). Second, the information in question could easily be recalled or obtained subsequently by the defendants. *Id.* at 607.

Moreover, an employee who changes employers or starts his own company cannot be prosecuted under the EEA merely on the ground that he was exposed to a trade secret while employed. Rather, the government must establish that he actually stole or misappropriated a particular trade secret, or at least that he conspired or attempted to do so.

IV.B.3.a.iii. Specification of Trade Secrets

The government should ascertain which specific information the victim claims as a trade secret early on. "[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 IV.C.2. of this Chapter).

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 (9th Cir. 2006).

IV.B.3.a.iv. Novelty

Unlike patents or copyrights, which require higher degrees of novelty, trade secrets must possess only "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 Arco Indus. Corp. v. Chemcast Corp.*, 633 F.2d 435, 442 (6th Cir. 1980) (same).

In other words, a trade secret must contain some element that is not known and that sets it 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, e.g., 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).

IV.B.3.a.v. 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). The "public" may not necessarily mean the general public. "[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). 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 will 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 would probably not qualify as "readily ascertainable 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. *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."); *Marshall v. Gipson Steel*, 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 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); *Buffets, Inc. v. Klinke*, 73 F.3d 965, 968 (9th Cir. 1996) (holding restaurant chain's recipes not to be trade secrets because, although innovative, the recipes were readily ascertainable by others).

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 Metallurgical Indus., Inc. v. Fourtek, Inc.*, 790 F.2d 1195, 1202 (5th Cir. 1986); *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 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.

IV.B.3.a.vi. Disclosure's Effects

A trade secret can lose its protected status through disclosure. To prove secrecy, the government often has the difficult burden of proving a negative, i.e., that the information was not generally available to the public. For this reason, the prosecutor should ascertain early on whether the purported trade secret was ever disclosed and to what extent those disclosures affect the information's status as a trade secret. These issues are covered thoroughly in Donald M. Zupanec, Annotation, *Disclosure of Trade Secret as Abandonment of Secrecy*, 92 A.L.R.3d 138 (2005) and

1 Roger M. Milgrim, *Milgrim on Trade Secrets* §§ 1.05-1.06 (2005). 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 times 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)). 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.* (citing *A.O. Smith Corp. v. Petroleum Iron Works Co.*, 73 F.2d 531, 537 (6th Cir. 1934)); 37 C.F.R. § 1.14, 35 U.S.C.A. App. I, at 653); *see also On-Line Techs. v. Perkin-Elmer Corp.*, 253 F. Supp. 2d 313, 323-27 (D. Conn. 2003). In return for the disclosure, the owner enjoys patent protection against other companies' use of the technology. 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).

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. v. Hillsborough County, Fla.*, 54 F. Supp. 2d 1300, 1303-04 (M.D. Fla. 1999); *Religious Tech. Ctr. v. Netcom On-Line Communication Servs.*, 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*, 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 certain circumstances. *See, e.g.*, *United States v. Lange,* 312 F.3d 263, 266 (7th Cir. 2002) (EEA case); *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 177 (7th Cir. 1991). For the security measures the trade secret owner must take to maintain secrecy during those disclosures, see Section IV.B.3.a.vii. 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.*, 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 does not, however, 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 does 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*, 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 IV.D.2. Section 1835 gives "a clear indication from Congress that trade secrets are to be protected to the fullest extent during EEA litigation." *United States v. Hsu*, 155 F.3d 189, 197 (3d Cir. 1988). 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 (2005).

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). "[T]o 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. v. Netcom On-Line Communication Servs.*, 923 F. Supp. at 1256.

IV.B.3.a.vii. Reasonable Measures to Maintain Secrecy

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); *United States v. Lange*, 312 F.3d 263, 266 (7th Cir. 2002). 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 cannot be convicted (at least under the EEA) for stealing the bicycle's design plans if the victim left the plans in a public park.

For these reasons, prosecutors should determine what measures the victim used to protect the trade secret. These protections will be a critical component of the case or the decision not to prosecute.

Typical security measures include:

- keeping the secret physically secure in locked drawers, cabinets, or rooms
- restricting access to those with a need to know
- restricting visitors to secret areas
- requiring recipients to sign confidentiality, nondisclosure, or noncompetition agreements
- marking documents as confidential or secret
- encrypting documents
- protecting computer files and directories with passwords
- splitting tasks among people or entities to avoid concentrating too much information in any one place

See 1 Roger M. Milgrim, *Milgrim on Trade Secrets* § 1.04 (2005); *Lange*, 312 F.3d at 266 (EEA case concerning aircraft brake assemblies); *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 521 (9th Cir. 1993) (discussing steps to safeguard computer system manufacturer's trade secrets from computer servicing company); *Reingold v. Swiftships, Inc.*, 126 F.3d 645, 650 (5th Cir. 1997) (discussing steps to protect ship-builder's mold for fiberglass boat hulls).

The owner's security measures need not be absolutely airtight. Rather, they must be reasonable under the facts of the specific case. *See* H.R. Rep. No. 104-788, *reprinted in* 1996 U.S.C.C.A.N. 4021, 4026, 4031; *Lange*, 312 F.3d at 266. *See also* 1 *Milgrim on Trade Secrets* § 1.04; *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); *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, nondisclosure, or noncompetition agreement was reasonable "in light of the close personal relationship enjoyed over the years" by the parties).

Information might not qualify as a trade secret if any low-level employee in a large company could access it. The theft of relatively unprotected information might, however, be prosecuted under a different statute. See Section IV.F. of this Chapter.

If the 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.*, *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.*, 923 F. Supp. at 1254. However, where the trade secret owner "rel[ies] 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 is 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 victims' 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 258 (S.D.N.Y 2005) (rejecting void-for-vagueness challenge to EEA indictment). *But see*

id. (noting that the defendant could argue that he was unaware of the victim's security measures at trial).

IV.B.3.a.viii. 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 jurisdictional level of value, the government must prove that the secret had 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 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).

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 Lange*, 312 F.3d at 269; *Genovese*, 409 F. Supp. 2d at 257. For more on methods of proving a trade secret's specific value, see Section VIII.C.2. of this Manual.

Not all of a business's confidential information is valuable in a competitor's hands. For example, in *Microstrategy v. Business Objects*, 331 F. Supp. 2d 396, 421 (E.D. Va. 2004), the court found that a company-wide e-mail 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 714 (finding no evidence of economic value without evidence that disclosure would have harmed the victim).

IV.B.3.a.ix. Example: Customer Lists

Some information that a company deems proprietary will 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, and 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 customer files of thousands of customers nationwide who were identified through a complex computer system to be trade secrets); *Electro Optical Indus., Inc. v. White*, 90 Cal. Rptr. 2d 680, 684 (Cal. Ct. App. 1999); *Leo Silfen, Inc. v. Cream*, 278 N.E.2d 636, 639-41 (N.Y. 1972). Conversely, 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"); *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); *Nalco Chem. Co. v. Hydro Techs., Inc.*, 984 F.2d 801, 804 (7th Cir. 1993) (holding that customer lists were not a trade secret when base of potential customers was neither fixed nor small).

IV.B.3.b. Misappropriation

IV.B.3.b.i. Types of Misappropriation

Under either § 1831 or § 1832, the defendant must have misappropriated the trade secret through one of the acts prohibited in § 1831(a)(1)-(5) or § 1832(a)(1)-(5). Misappropriation covers a broad range of acts. It includes not only traditional methods of theft in which a trade secret is physically removed from the owner's possession, but also less traditional methods of misappropriation and destruction 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 misappropriated trade secrets. *See* 18 U.S.C. §§ 1831(3), 1832(3).

IV.B.3.b.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.*, 4 Roger M. Milgrim, *Milgrim on Trade Secrets* § 15.01[e]; *Stampede Tool Warehouse 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). Trade secret cases to the contrary that do not involve the EEA are thus 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 "mental recollections" and a defense that "great minds think alike."

IV.B.3.b.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.B.3.b.iv. Misappropriation of Only Part of a Trade Secret

The defendant can be prosecuted even if he misappropriated only part of the 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 that "what matters is how important the documents [the defendant] had were to [the defendant], not their number").

IV.B.3.b.v. Mere Risk of Misappropriation Not Prosecutable, But Attempts and Conspiracies Are

However, 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 actually stole or misappropriated a particular trade secret or that she attempted or conspired to do so.

IV.B.3.c. Knowledge

The first mens rea element in an EEA case is that the defendant misappropriated the trade secret "knowingly." Section 1831(a) applies to anyone who misappropriates a trade secret "knowingly." Section 1832(a), by contrast, applies to "[w]hoever, with intent to convert a trade secret," engages in misappropriation. This is a distinction without a difference, because knowing misappropriation is equivalent to the intent to convert.

"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). Because criminal statutes covering the theft of tangible property generally require the government to prove that the defendant "[knew] that the object he [stole was] indeed a piece of property that he [had] no lawful right to convert for his personal use," the government generally must show that the defendant knew or had a firm belief that the information he or she was taking was a trade secret in an EEA case as well. 142 Cong. Rec. 27,117 (1996) (EEA legislative history). *See United States v. Genovese*, 409 F. Supp. 2d 253, 258 (S.D.N.Y. 2005) (discussing alleged circumstances that would indicate that EEA defendant knew the information was a trade secret).

Ignorance of the law is no defense. The government need not prove that the defendant himself had concluded that the information he took fit the legal definition of a "trade secret" set forth in 18 U.S.C. § 1839(3). If the government had to prove this, EEA violations would be nearly impossible to prosecute and Congress's intent would be contravened:

> This [knowledge] requirement should not prove to be a great barrier to legitimate and warranted prosecutions. Most companies go to considerable pains to protect their trade secrets. Documents are marked proprietary; security measures put in place; and employees often sign confidentiality agreements.

142 Cong. Rec. 27,117 (1996). Based on this legislative history, the government should be able to establish that the defendant knew that the information was a trade secret by proving that he was aware that the information was protected by proprietary markings, security measures, and confidentiality agreements. *Id.* More generally, the government could simply prove that the defendant knew or had a firm belief that the information 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 18 U.S.C. § 1839(3). *Cf. Genovese*, 409 F. Supp. 2d at 258 (discussing alleged circumstances that would indicate that EEA defendant knew the information was a trade secret). On the other hand, a person cannot be prosecuted under the EEA if "he [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.*

IV.B.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." 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 tied to a foreign government. See Section IV.B.3.c. of this Chapter. 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." 142 Cong. Rec. 27,116 (1996).

The "benefit" to the foreign entity should be interpreted broadly. It is not limited to an economic benefit, but rather also includes a "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 its use suggests 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 foreign corporation that acted without the sponsorship of, or "coordinated intelligence activity" by, a foreign government. *Id.* In such an instance, however, the foreign corporation could still be properly charged under 18 U.S.C. § 1832.

For questions concerning charges under § 1831, contact the Department's Counterespionage Section at (202) 514-1187 or CCIPS at (202) 514-1026.

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

IV.B.5.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).

IV.B.5.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 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4023. 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

(1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4030 ("[M]isappropriation effectively destroys the value of what is left with the rightful owner."). Most employees understand that their misappropriation will injure the victim once he loses the exclusive use of his trade secret.

IV.B.5.c. Product Produced for or Placed in Interstate or Foreign Commerce

On a charge of domestic economic espionage under 18 U.S.C. § 1832, the government must prove that the trade secret was "related to or included in a product that is produced for or placed in interstate or foreign commerce." 18 U.S.C. § 1832; *compare* 18 U.S.C. § 1831 (containing no explicit language about being included in or related to a product).

The defendant need not have known that the trade secret was related to or included in a product that was produced for or placed in interstate or foreign commerce. The nexus to interstate or foreign commerce appears to have been intended merely to allow federal jurisdiction. 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 produced for or placed 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, if the product is still being developed, § 1832 would merely require proof that the trade secret was "related to ... a product that is produced for ... interstate or foreign commerce." 18 U.S.C. § 1832(a). A defendant might argue that a product still in the research and development stage is not yet being "produced for ... interstate commerce," 18 U.S.C. § 1832, because the prototype itself is not being "produced" 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.

To prove that the product was produced for interstate or foreign commerce, the government need only show the victim's intent to

distribute the product or utilize the process under development for a product. This can be demonstrated through evidence of the project's goals.

At this writing, the only published case concerning these issues is *United States v. Yang*, 281 F.3d 534, 551 & n.4 (6th Cir. 2002), which 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.

This element implicitly distinguishes between the misappropriation of trade secrets related to products—which is punishable under § 1832—and trade secrets related to services—which is not. For criminal charges to consider when the trade secret is related to services, see Section IV.F. of this Chapter.

Distinguishing when a trade secret relates to a product and when it relates to a service is sometimes easier said than done. Although the "product" requirement is not discussed in the legislative history, the term's plain meaning appears to exclude pure services such as technical skills and know-how that are not embodied in or related to a saleable, transportable good. Consider a chiropractor's secret technique to treat back pain by manipulating a patient's spine. If the chiropractor is not developing and has not developed a medical product that uses or embodies the secret, but instead merely uses the technique in private practice, the technique's theft by a coworker or common thief would not violate § 1832. By contrast, cellular telephone companies sell services that are accompanied by a "free" cellular phone or require the purchase of a compatible phone. If a cellular company develops a trade secret relating to the technical operation of its cellular network, the fact that the essence of what the company provides is a service should not necessarily preclude a prosecution under the EEA, given that the secret could be categorized as being "related to ... a product [the phone] that is produced for or placed in interstate or foreign commerce." §1832(a).

IV.B.6. Attempts and Conspiracies, Including the Impossibility Defense

As noted, the EEA—both foreign and domestic—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. *United States v. Hsu*, 155 F.3d 189, 202 (3d Cir. 1998). 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).

In *Hsu*, the Sixth Circuit ruled that to convict a defendant under the EEA of attempt or conspiracy, the government need not prove that the information the defendant sought actually constituted a trade secret. *Hsu*, 155 F.3d at 204.

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). 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 203-04.

The government need not prove the existence of an actual trade secret, 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." *Id.* at 203. 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.*

The Third Circuit also 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 evidenced 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, 542-45 (6th Cir. 2002), *cert. denied*, 537 U.S. 1170 (2003), and the Seventh Circuit in *United States v. Lange*, 312 F.3d 263, 268-69 (7th Cir. 2002).

IV.C. Defenses

IV.C.1. Parallel Development

According to the EEA's legislative history, 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.*

IV.C.2. Reverse Engineering

Similarly, a person may legally discover the information underlying a trade secret by "reverse engineering," that is, the practice of taking something apart 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[d][iv]; *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"); *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.

IV.C.3. Impossibility

The defense of impossibility has largely been rejected by courts in EEA prosecutions. See Section IV.B.6. of this Chapter.

IV.C.4. Advice of Counsel

"There is no such thing as an 'advice of counsel' defense." *United States v. Urfer*, 287 F.3d 663, 666 (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.* 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 Section IV.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. *See* Section IV.C.5.

To rely on advice of counsel 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); *see also United States v. Butler*, 211 F.3d 826, 833 (4th Cir. 2000) (same).

IV.C.5. Claim of Right—Public Domain and Proprietary Rights

As is discussed in Section IV.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 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 Section IV.B.3.a.vi. (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 IV.C.4. of this Chapter. Notwithstanding the passage of the EEA, many disputes about trade secrets are still best resolved in a civil forum.

IV.C.6. The First Amendment

The First Amendment is 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*, 75 P.3d 1, 19 (Cal. 2003) ("We merely hold that the preliminary injunction does not violate the free speech clauses of the United States and California Constitutions, *assuming* the trial court properly issued the injunction under California's trade secret law. On remand, the Court of Appeal should determine the validity of this assumption.").

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*.

IV.C.7. 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 on numerous grounds.

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. 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 "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 preventing 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 e-mails, 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.

Subsequent courts have ruled similarly. *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. 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). *But see id.* at 258 (stating further that

the defendant could argue that he could not have known the victim's protective measures at a later stage of the proceedings).

IV.D. Special Issues

IV.D.1. Civil Injunctive Relief for the United States

The EEA authorizes the government to file a civil action seeking injunctive relief. *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 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).

IV.D.2. Confidentiality and the Use of Protective Orders

Victims of trade secret theft are often conflicted about whether to report these thefts to law enforcement authorities. They want the thief to be punished, but worry that their trade secret would be disclosed during discovery or trial.

Congress resolved this dilemma by giving the government measures to preserve the confidentiality of trade secrets throughout the prosecution. 142 Cong. Rec. 27,105 (1996). The EEA provides that the 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." 18 U.S.C. § 1835. The government has the right to an interlocutory appeal from an order authorizing a trade secret's disclosure. *Id.*; *see also United*

States v. Ye, 436 F.3d 1117, 1120-24 (9th Cir. 2006) (discussing extent and limits to interlocutory appeal 18 U.S.C. § 1835 and when mandamus relief in an EEA discovery dispute may be ordered under 28 U.S.C. § 1651).

Prosecutors are therefore strongly encouraged to move the court to take such actions as necessary and appropriate to prevent the trade secret's harmful disclosure. There are a number of ways to accomplish this. Protective orders can limit the amount or degree of disclosure in discovery, permit *in camera* review by the court prior to disclosure, allow or require the submission of redacted documents and sealed exhibits, and allow or require the use of courtroom video monitors to display documents to counsel, the court, and the jury, but not to the public. *See, e.g., 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); *Skolnick v. Altheimer & Gray*, 730 N.E. 2d 4, 14 (Ill. 2000) (holding that trial court abused its discretion by refusing to modify a protective order that allowed parties to designate information disclosed in discovery as "confidential").

The use of protective orders was endorsed in *United States v. Hsu*, 155 F.3d 189, 197 (3d Cir. 1998). In the district court, the government moved under 18 U.S.C. § 1835 and Fed. R. Crim. P. 16(d)(1) for a protective order to limit the government's production of documents used in the sting operation to redacted copies of documents relating to the trade secrets at issue. *United States v. Hsu*, 982 F. Supp. 1022, 1023 (E.D. Pa. 1997). The defendants wanted unredacted copies, but were willing to stipulate that they would use the documents only in the criminal litigation and would return or destroy the documents at the case's end. The district court agreed with the defendants' need for unredacted documents. *Id.* at 1029-30.

On the government's interlocutory appeal, the Third Circuit held that 18 U.S.C. § 1835 clearly demonstrates Congress's intent to protect the confidentiality of trade secrets to the fullest extent possible under the law. *Hsu*, 155 F.3d at 197. While recognizing that such protection does not abrogate criminal defendants' constitutional and statutory rights, the court held that the government's proposed order to produce only redacted copies of the targeted documents did not violate the defendants' constitutional rights 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," and the actual trade secret documents were

irrelevant to that inquiry. *Id.* at 203. Because the indictment did not charge a completed theft, the Third Circuit refrained from addressing the district court's conclusion that in a case charging a completed offense, actual trade secrets must be disclosed to defendants. The Third Circuit characterized this question as "complex," noting that the EEA's definition of trade secret "raises an issue as to whether the information or formula itself is in fact material to the existence of the trade secret." *Id.* at n.15. Thus, the limits of the government's ability to restrict disclosure in a criminal case concerning a completed offense have not yet been addressed.

As to the defendants' claim that they needed to see the trade secrets to prepare their other defenses, including entrapment and outrageous government conduct, the Third Circuit skeptically remanded these issues to the district court. *Id.* at 205. On remand, the district court held that the defendants were not entitled to receive unredacted trade secret documents under Fed. R. Crim. P. 16(a)(1)(C), and found the unredacted documents to be irrelevant to the defenses of entrapment and outrageous government conduct. *United States v. Hsu*, 185 F.R.D. 192, 198 n.19 (E.D. Penn. 1999). Just as a drug defendant needs no access to the drugs to allege entrapment, neither does an EEA defendant need access to the trade secrets to do the same. *Id.*

The court similarly rejected the defendants' arguments for full disclosure based on the defenses of document integrity and chain of custody. *Id.* at 199 (concluding that those defenses could "be resolved at a later date without the defense viewing the redacted information ... just as chain of custody questions in drug or gun prosecutions can be resolved without having to touch the objects themselves" as well as the claims that the government and Bristol-Meyers waived the confidentiality of the trade secrets when they showed the documents voluntarily during the sting operation).

Finally, the court disagreed that the unredacted documents could help the defendants prove that the documents' information was in the public domain. After *in camera* review by a court-appointed technical advisor who had taken an oath of confidentiality, the court concluded that the largest category of redactions, consisting of "specific examples of experimental conditions," satisfied the statutory definition of a trade secret contained in 18 U.S.C. § 1839(3). After reviewing this category of redactions *in camera* and consulting with the expert, the court held that the redactions were proper to avoid disclosure of trade secrets. *Id.* at 200. The court did, however, order the disclosure of certain redacted information that fell outside the EEA's definition of a trade secret. *Id.*

Taken together, the appellate and trial courts' opinions in *Hsu* suggest that courts will recognize and respect Congress's directive to preserve the confidentiality of trade secrets throughout the criminal process.

Before trial, the defense has no right to take 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 (9th Cir. 2006).

During trial, courts can limit the public disclosure of information without violating the defendant's right to a public trial under the Sixth Amendment. The right to a public criminal trial is not absolute and may be limited in certain circumstances. *See Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 599-600 (1980) (Stewart, J. concurring); *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); *State ex rel. La Crosse Tribune v. Circuit Court*, 340 N.W.2d 460, 466-67 (Wis. 1983) (discussing court's inherent power to limit the public nature of trials).

Before requesting that a courtroom be sealed, prosecutors should comply with the procedures in the federal regulations and Department of Justice guidelines requiring the Deputy Attorney General's prior approval. *See* 28 C.F.R. § 50.9; USAM 9-5.150. The regulations create a strong presumption against sealing courtrooms and provide for such action "only when a closed proceeding is plainly essential to the interests of justice." 28 C.F.R. § 50.9. A prosecutor who wants to close a judicial proceeding in a case or matter under the supervision of the Criminal Division should contact the Criminal Division's Policy and Statutory Enforcement Unit, Office of Enforcement Operations at (202) 305-4023. In cases or matters supervised outside of the Criminal Division, the prosecutor should contact the supervising division. USAM 9-5.150.

For a helpful discussion of the use of protective orders in civil cases and a collection of relevant cases, see 3 Roger M. Milgrim, *Milgrim on Trade Secrets* § 14.02[5]-[7].

IV.D.3. 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.

IV.D.4. Department of Justice Oversight

Before Congress passed the EEA, the Attorney General promised that all EEA prosecutions during the EEA's first five years would be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General of the Criminal Division. 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.

The approval requirement for § 1832 prosecutions lapsed after the five-year period expired on October 11, 2001, so 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.

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 Criminal Division, through the Counterespionage Section. USAM 9-2.400, 9-59.000. The Counterespionage Section can be reached at (202) 514-1187..

IV.E. Penalties

IV.E.1. Statutory Penalties

IV.E.1.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 $500,000 or twice the monetary gain or loss, or both, 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)(4), 1832(a)(5). 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).

IV.E.1.b. Criminal Forfeiture

The EEA provides criminal forfeiture. It directs that the sentencing court

> shall order ... that the person forfeit to the United States—
>
> (1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and
>
> (2) any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.

18 U.S.C. § 1834(a). Forfeiture of proceeds is mandatory, while forfeiture of instrumentalities is discretionary. 18 U.S.C. § 1834(a)(1)-(2).

As a procedural matter, the government should allege forfeiture in the indictment. For additional discussion of forfeiture in intellectual property infringement cases, see Chapter VIII of this Manual.

IV.E.1.c. Restitution

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).

The theft of trade secrets meets § 3663A's definition of property offenses that require restitution. Section 3663A's legislative history indicates that restitution is required in "violent crimes, *property* and *fraud* crimes under title 18, product tampering, and certain drug crimes." S.

Rep. No. 104-179, at 14 (1995), *reprinted in* 1996 U.S.C.C.A.N. 924, 927 (emphasis added). The misappropriation of trade secrets is essentially the theft of property. *Cf. Carpenter v. United States*, 484 U.S. 19, 28 (1987) (holding that newspaper's confidential information qualified as "property"); *Matter of Miller*, 156 F.3d 598, 602 (5th Cir. 1998) (defining misappropriation of proprietary information as the "wrongful taking and use of another's property"); *Westinghouse Elec. Corp. v. U.S. Nuclear Regulatory Comm'n*, 555 F.2d 82, 95 (3d Cir. 1977) (describing "property in the form of its proprietary information"). Accordingly, the theft of trade secrets should qualify as an "offense against property" under § 3663A for which the defendant must make restitution.

As noted, the mandatory restitution statute also applies to any offense where "an identifiable victim 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 intellectual property infringement cases, see Chapter VIII of this Manual.

IV.E.2. Sentencing Guidelines

Issues concerning the sentencing guidelines are covered in Chapter VIII of this Manual.

IV.F. Other Charges to Consider

When confronted with a case that implicates confidential proprietary information, prosecutors may wish to consider the following crimes in addition to or in lieu of EEA charges:

- **Disclosing government trade secrets, 18 U.S.C. § 1905**, which punishes government employees and contractors who, *inter alia*, "divulge" or "disclose" government trade secrets. *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.

- **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, pt. IV(1)(B), 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).

- **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).

- **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 to deprive them of the intangible right of honest services, which often cover the misappropriation of 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 under both theories).

First, 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).

Second, a scheme to defraud may include the defendant's deprivation of the victim's intangible right to the defendant's honest services, under 18 U.S.C. § 1346. Under § 1346, the defendant is charged not with fraudulently obtaining proprietary information, but rather with breaching his fiduciary duty of loyalty to his employer by misappropriating the proprietary information. *Id.* The government need not, however, prove that the defendant realized financial gain from the theft or attempted theft. *See, e.g., United States v. Kelly*, 507 F. Supp. 495 (E.D. Pa. 1981) (holding that a private employee may be convicted for mail fraud for failing to render honest and faithful services to his employer if he devises a scheme to deceive, mislead, or conceal material information, in case where the defendants violated their employer's policy by extensively using the employer's computer facilities for their own gain and had attempted to conceal their actions from the employer). Section 1346 covers all employees, not just those who work for a government. *See United States v. Martin*, 228 F. 3d 1, 17 (1st Cir. 2000); *United States v. Frost*, 125 F.3d 346, 365 (6th Cir. 1997).

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, 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).

For a more detailed discussion of 18 U.S.C. §§ 1341 and 1343, refer to Title 9, Chapter 43 of the U.S. Attorneys' Manual, 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 International Transportation of Stolen Property Act (hereinafter "ITSP 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**.

  At least one court has held that the ITSP Act does not apply to the theft of trade secrets or other proprietary and confidential information unless the information is of a type bought, sold, or transferred in a legitimate or black market. In an unpublished district court opinion, the court held that "goods," "wares," and "merchandise" do not include every item "related to commerce," but rather only "those things that are bought and sold in the marketplace." *United States v. Kwan*, No. 02 CR.241 (DAB), 2003 WL 22973515, at *6 (S.D.N.Y. Dec. 17, 2003). Because the government had not proved that the victim's travel industry "proprietary information includ[ing] hotel contact lists, hotel rate

sheets, travel consortium contact lists, travel consortium rate sheets, and cruise operator rate sheets," were the type of goods, wares, or merchandise that were ever bought, sold, or traded in a market, "legal or otherwise," the *Kwan* court vacated the defendant's ITSP conviction. *Id.* at *1, *6.

Assuming that particular stolen items qualify as goods, wares, or merchandise, the courts agree that sections 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 [ITSP] 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 ITSP 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 ITSP Act. *See also supra* Chapter II.F. (discussing application of *Dowling* to charging 18 U.S.C. § 2314 for intellectual property crimes).

The Second Circuit reached the opposite result in *United States v. Bottone*, 365 F.2d 389 (2d Cir. 1966), which pre-dates *Dowling*. The defendants in *Bottone* removed papers describing manufacturing processes from their place of employment and made copies outside the office. They returned the originals and then transported the copies in interstate commerce. In upholding defendants' convictions under 18 U.S.C. § 2314, Judge Friendly stated that:

> when the physical form of the stolen goods is secondary in every respect to the matter recorded in them, the transformation of the information in the stolen papers into a tangible object never possessed by the original owner should be deemed immaterial. It would offend common sense to hold that these defendants fall outside the statute simply because, in efforts to avoid detection, their confederates were at pains to restore the original papers to [their employer] and transport only copies or notes, although an oversight would have brought them within it.

365 F.2d at 393-94.

More recent cases have adopted similar reasoning, notwithstanding *Dowling* and *Brown*, approving of ITSP prosecutions for theft of

intangible property by intangible means. *See, e.g.*, *United States v. Kwan*, No. 02 CR.241 (DAB), 2003 WL 21180401, *3 (S.D.N.Y. 2003) (denying the defendant's motion to dismiss, because in determining what would be considered "goods, wares, or merchandise," the Second Circuit "long considered stolen items' commercial nature to be more significant than their tangibility."); *United States v. Farraj*, 142 F. Supp. 2d 484, 488 (S.D.N.Y. 2001) ("The text of § 2314 makes no distinction between tangible and intangible property, or between electronic and other manner of transfer across state lines."); *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.").

- State and local charges. Many states have laws that specifically address the theft of information. If a state lacks a specific trade-secret law, its general theft statutes may apply.

V.

Digital Millennium Copyright Act— 17 U.S.C. §§ 1201-1205

V.A. Introduction

V.A.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, 454 (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.

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 V.B.5. of this Chapter.

V.A.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 V.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). (At this writing, the reference to § 118(g) at § 1204(b) has not been amended to indicate the provision's current location at § 118(f).)

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.

V.A.2.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 Web site 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). 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 Web site 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 Web site 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 Web site 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. A district court in the Northern District of California, however, viewed the same technology as both an access control and a copy control. *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.

V.A.2.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 V.B.1. and V.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. 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).

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)

V.A.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). 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*, 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.").

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); *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"). 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 V.B.1.c. of this Chapter.

V.A.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.

V.B. Elements of the Anti-Circumvention and Anti-Trafficking Provisions

V.B.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 recent 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 Technology 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 V.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 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 V.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.

V.B.1.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.

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. *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 Egilman*, 401 F. Supp. 2d at 113-14; *I.M.S.*, 307 F. Supp. 2d at 531-33. 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.

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"). *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.

V.B.1.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). 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*; *see also 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"). 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. *Id.* 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.* (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") *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).

V.B.1.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).

V.B.1.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 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*, Civ. No. 2:99CV02070, 2000 WL 127311, at *3 (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.

V.B.1.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). 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, effective from October 28, 2003, until October 27, 2006, are

- compilations containing lists of blocked Web sites intended to prevent access to domains, Web sites, or portions of Web sites (but not lists of Internet locations blocked by software designed to protect against damage to computers, such as firewalls and antivirus software, or software designed to prevent receipt of unwanted e-mail, such as anti-spam software).

- computer programs protected by dongles—security or copy protection devices for commercial microcomputer programs—that prevent access due to malfunction or damage and which are obsolete.
- "computer programs and video games distributed in formats that have become obsolete and th[at] require[] original media or hardware as a condition of access."
- "literary works distributed in e-book format when all existing e-book editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling of the e-book's read-aloud function and that prevent the enabling of screen readers to render the text into a 'specialized format.'"

See 37 C.F.R. § 201.40 (2003). The next rulemaking will occur in 2006.

V.B.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 V.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 V.B.1.

V.B.2.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). 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 Web sites 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.

V.B.2.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*, 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).

V.B.2.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. 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. Streambox, Inc.*, No. 2:99CV02070, 2000 WL 127311, at *8 (W.D. Wash. Jan. 18, 2000).

V.B.2.c.1. 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), and copyrighted movies encrypted onto DVDs (*Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 318-19 (S.D.N.Y. 2000); *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1098 (N.D. Cal. 2004)).

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. The defendant's subjective motive may, however, affect whether his conduct falls within one of the DMCA's statutory exceptions. See Section V.C. of this Chapter.

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.* The trafficking "of the program is the prohibited conduct—and it is prohibited irrespective of why the program was written." *Id.*

V.B.2.c.2. 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.

V.B.2.c.3. 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 V.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).").

V.B.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 V.B.1. and V.B.2. of this Chapter.

V.B.3.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*, 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); and (3) 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 one court has held that an unlicensed DVD player that can bypass 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.

V.B.3.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, limits or

otherwise restricts the exercise of any of the rights set forth in [§] 106." *See id.* at 1124; *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. 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); *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. 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.

V.B.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).

V.B.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.

V.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)).

V.C.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).

V.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 V.B.1.e. of this Chapter.

V.C.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.

V.C.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. 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 id.* at 66.

V.C.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). 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) (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 & Assoc. Inc. v. Internet Gateway, Inc.*, 334 F. Supp. 2d 1164, 1185-86 (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 by 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").

V.C.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).

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 is 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.

V.C.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.

V.C.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.

V.C.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).

V.C.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.

V.C.10.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*, 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. 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's 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 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.*

V.C.10.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.

V.C.10.b.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.

V.C.10.b.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). The government's purpose is the controlling measure. *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989).

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).

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 V.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.

V.C.10.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. *Id.* 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 id.*; 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).

V.C.10.d. Fair Use

For a more detailed explanation of the fair use doctrine, see Section II.C.5. 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. Thus, the DMCA's anti-trafficking provisions are not concerned with purchasers' downstream use of circumvention tools. *See Corley*, 273 F.3d at 442; *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.

V.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 both. 17 U.S.C. § 1204. For subsequent offenses, each of those punishments can be doubled. *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

VI.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 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, the use of a counterfeit trademark is not necessarily an element of a § 2318 charge. And although the counterfeit marks statute, 18 U.S.C. § 2320, criminalizes the use of counterfeit labels that bear counterfeit trademarks, § 2320 covers counterfeit labels that accompany any kind of trademarked product or service, and not just the types of copyrighted works covered by § 2318.

Several important amendments to § 2318 went into effect on December 23, 2004 and March 16, 2006. See Sections VI.B.2, VI.B.3, and VI.E.5.a. of this Chapter. As a result of the 2004 amendments, § 2318 now covers counterfeit labels not only for movies, music, and software, but for other types of copyrighted works as well, namely, copies of literary, pictorial, graphic, or sculptural works, works of visual art, and documentation and packaging for any of the enumerated classes of copyrighted works. 18 U.S.C. § 2318(a)(1). The 2004 amendments also expanded § 2318 to cover counterfeit documentation and packaging itself for the newly-added classes of works. 18 U.S.C. § 2318(a)(2). The section

also now covers the new category of 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 (that is, 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). The 2006 amendments expanded the definition of "traffic" to include a wider variety of profit-oriented conduct, and directed the Sentencing Commission to study the guidelines concerning labels, with guideline amendments expected later in 2006. See Sections VI.B.2. and VI.E.5.a. of this Chapter.

Sample indictments and jury instructions are provided in Appendix F of this Manual.

VI.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.

VI.B.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, in which the government often must prove that the defendant knew that he acted illegally (see the discussion of the "willful" standard in criminal copyright infringement cases in Chapter II of this Manual). Proving knowledge under § 2318 only requires proof that the defendant knew that he was taking the actions described in the statute. *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.").

The government need not prove that the defendant acted with fraudulent intent in § 2318 cases involving counterfeit labels. 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.

What, then, must the government prove that the defendant knew? Clearly, the government must prove the defendant knowingly trafficked in labels, documentation, or packaging, but this will generally be easy to show.

The crux is to prove that the defendant knew that the labels, documentation, or packaging in which he trafficked were counterfeit or illicit, as the case may be. *See, e.g., United States v. Dixon*, No. 84-5287, 1985 U.S. App. LEXIS 27076, at *9 (4th Cir. Aug. 12, 1985).

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, 699-705 (9th Cir.) (discussing the history and use of "deliberate ignorance" instructions); *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." *See 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 the jurisdictional elements listed in § 2318(c) fit his conduct, such as that the computer program to which he had affixed his counterfeit labels was copyrighted. See Section VI.B.5. of this Chapter.

VI.B.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. This element was significantly changed on March 16, 2006 by the Protecting American Goods and Services Act of 2005, Pub. L. No. 109-181, § 2, 120 Stat. 285, 288 (March 16, 2006).

Before the March 16, 2006 amendments, "traffic" was statutorily defined within § 2318 to mean "to transport, transfer or otherwise dispose of, to another, as consideration for anything of value or to make or obtain control of with intent to so transport, transfer or dispose of." 18 U.S.C. § 2318(b)(2). Congress defined "traffic" specifically to exclude individuals who knowingly acquire counterfeit labels or other articles solely for personal use. *See* S. Rep. No. 97-274, at 9 (1981), *reprinted in* 1982 U.S.C.C.A.N. 127, 135. This definition was identical to the definition of "traffic" in 18 U.S.C. § 2320(e)(2) ("Trafficking in counterfeit goods or services")—before that definition was also changed in the 2006 act—with the same issues concerning what qualified as "consideration" and what did not, as well as the issues concerning possession with intent to traffic. See Section III.B.3.b. of this Manual.

The March 16, 2006 amendments made the parallels between the two statutes' definition of "traffic" more explicit. For cases arising from conduct on or after that date, the definition of "traffic" in § 2318(b)(2) has been amended to read, "the term 'traffic' has the same meaning as in section 2320(e) of this title [18]." Protecting American Goods and Services Act of 2005, § 2(c)(2), 120 Stat. at 288 (amending 18 U.S.C. § 2318(b)(2)). As is discussed in Section III.B.3.b. of this Manual, these amendments deal with the issues concerning consideration and possession with intent to traffic.

Prosecutors should therefore consult Section III.B.3.b., which covers the counterfeit marks crime in 18 U.S.C. § 2320, for a discussion of how the traffic element operated before and after the March 16, 2006 amendments. The only differences to be noted are 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, the definition of "traffic" in both statutes now includes so many acts that are preparatory to distributing contraband—such as making it, obtaining it, and possessing it with intent to traffic—that the omission of an attempt provision in § 2318 should not prevent the government from otherwise pursuing 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.

VI.B.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 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)

Before 2004, § 2318 prohibited trafficking in counterfeit labels designed to be affixed to phonorecords, copies of computer programs, motion pictures and audiovisual works, and counterfeit documentation and packaging for computer programs. In 2004, Congress extended § 2318 substantially as part of the Intellectual Property Protection and Courts Amendment Act of 2004, Pub. L. No. 108-482, 118 Stat. 3912 (Dec. 23, 2004).

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), (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)-(2), (b)(5).

The types of copyrighted works covered by the statute has expanded significantly over the past several years. 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 governing computer software had only been added in 1996. Amendments in 2004 now expressly include labels, documentation, and packaging for phonorecords, motion pictures or other audiovisual works, computer software, literary, pictorial, graphic, or sculptural works, and works of visual art. *See* 18 U.S.C. § 2318(a)(1), (b)(5).

The 2004 amendments also changed slightly the actual or intended physical proximity of the labels and the copyrighted works for which they are intended. Before the 2004 amendments, § 2318 covered labels that had been "affixed or designed to be affixed to" certain works. 18 U.S.C. § 2318(a) (2003). "[D]esigned to be affixed" was included to cover counterfeit labels that had not actually been attached to a work: it was added to the statute to close a "loophole" in which some counterfeiters had shipped only unattached labels. *See* S. Rep. No. 97-274, at 9 (1981), *reprinted in* 1982 U.S.C.C.A.N. 127, 135. The physical nexus grew even broader with the 2004 amendments, which expanded "affixed or designed to be affixed" to "affixed to, enclosing, or accompanying, or designed to be affixed to, enclose, or accompany." 18 U.S.C. § 2318(a)(1). Despite this expansion, some physical nexus between the labels 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 VI.D.1. of this Chapter.

VI.B.4. The Labels, Documentation, or Packaging Materials Are Counterfeit or Illicit

In the fourth element, the government must prove that the packaging or documentation are "counterfeit" or that the labels are "counterfeit" or "illicit." *See* 18 U.S.C. § 2318(a)(1)-(2).

"Counterfeit" is defined as something "that appears to be genuine, but is not." 18 U.S.C. § 2318(b)(1), (b)(6). Counterfeit is distinct from "bootlegged" or "pirated": 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"), and 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). Although § 2318 was amended to

cover "illicit" labels on December 23, 2004, as of this writing there are no reported cases that involve illicit labels. For now, therefore, we must rely solely on the statute. 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.

VI.B.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, enclosed or accompanying or designed to be affixed, enclosed or to 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)

In practice, the most likely basis for jurisdiction will be copyright. However, even when the works are copyrighted, 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 copyright should be read as an element of these jurisdictional bases.

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 VI.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, 73 n.3 (1994) (affirming *Feola* as applied to strictly jurisdictional facts); *United States v. Yermain*, 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 willingly" to apply to jurisdictional element).

VI.B.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.

VI.C. Defenses: 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.

VI.D. Special Issues

VI.D.1. Electronic Copies of Labels, Documentation, or Packaging

Although a typical case under § 2318 generally involves labels, documentation, 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 cases when either the "original" or "legitimate" items, or the "counterfeit" or "illicit" copies, or both, are in electronic or digital form. However, such circumstances are limited. 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 would 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, as of this writing, there is little case law in this area, and the extent to which § 2318 may be applied in situations involving electronic labeling components remains somewhat unclear.

VI.D.2. Advantages of Charging a § 2318 Offense

A § 2318 charge may be an appropriate adjunct or alternative charge when the situation 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.

VI.E. Penalties

Section 2318(a) provides for a fine or imprisonment or both, as well as forfeiture. Restitution is also available.

VI.E.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).

VI.E.2. Imprisonment

The maximum term of imprisonment is five years. 18 U.S.C. § 2318(a).

VI.E.3. Restitution

Although § 2318 does not mention restitution, 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.

VI.E.4. Forfeiture

When a person is convicted under § 2318, the court must order the forfeiture and destruction or other disposition of all counterfeit or illicit labels, any items that these labels were affixed to or intended to be affixed to, and any equipment, device, or material used to create these labels. *See* 18 U.S.C. § 2318(d). For more on forfeiture, see Chapter VIII of this Manual.

VI.E.5. Sentencing Guidelines

Section 2B5.3 is the applicable sentencing guideline. See Chapter VIII of this Manual. Section 2318 offenses in particular often raise issues about how to evaluate the retail value and the number of infringing items on which to base the infringement amount.

VI.E.5.a. Retail Value of Copyrighted Goods vs. Counterfeit Labels, Documentation, and Packaging

The retail value may depend on whether the defendant's labels, documentation, and packaging were enclosed, affixed to, or accompanied the materials for which they were intended. If so, the infringement amount is calculated as usual, based on the retail value of the infringed (genuine) or infringing (counterfeit) copyrighted material as Application Note 2 to U.S.S.G. § 2B5.2 directs. See Chapter VIII of this Manual. If not, then determining an infringement amount for unattached labels, packaging, or documentation—standing alone—may be more complicated.

On March 16, 2006, the Stop Counterfeiting in Manufactured Goods Act directed the Sentencing Commission to address how the infringement amount should be calculated for offenses involving labels, documentation, and packaging, such as 18 U.S.C. § 2318, that are not attached to or accompanying copyrighted works. *See* Pub. L. No. 109-181, § 1, 120 Stat.

285 (March 16, 2006). Guideline clarifications pursuant to this directive are expected later in 2006, after this Manual goes to print.

Until the guidelines are clarified, at least one past decision indicates that unattached labels, documentation, and packaging be based on the retail value of the labels, documentation, or packaging themselves. 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.

The court might have used the $50 value of the software plus a manual had there been evidence that Bao understood the conspiracy to extend beyond counterfeit manuals to counterfeit software. *Id.* at 867 n.3. This logic may therefore apply in future cases when the counterfeit or illicit labels, documentation, or packaging have no retail value separate from the infringing copyrighted material, such as labels of Microsoft trademark that could be applied to Microsoft software. *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.").

The December 2004 amendments to § 2318 prohibiting traffic in "illicit" labels may also present some novel sentencing issues. Because "illicit" labels are genuine labels that are used beyond the authorized scope of the copyright holder, it may be difficult to determine the infringement value of illicit labels that have not actually been affixed to, enclosed with, or accompanied the copyrighted material. Since illicit labels are genuine and not counterfeit, should the retail value of the genuine label always be used to determine the infringement amount for sentencing purposes? It is not clear, particularly because there are no reported cases addressing trafficking in illicit labels. But the addition of illicit labels to

§ 2318 does blur the distinction between infringing (fake) and infringed (genuine) retail value for sentencing purposes.

VI.E.5.b. Number of Infringing Copyrighted Goods vs. Number of Labels, Documents, or Packaging Items

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 (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 the counterfeit trademark crime, 18 U.S.C. § 2320, not the counterfeit label crime in § 2318. It is difficult to predict how these issues will be resolved in § 2318 prosecutions, in which the focus is not the completed counterfeit product—as in § 2320 cases—but rather the counterfeit label, documentation, or packaging.

VI.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. 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 Section II.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 Racketeering 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 Section II.F. of this Manual.

VII.

Patent

VII.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 or 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). The federal government's authority to grant patents stems from U.S. Const. art. I, § 8, 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. 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. *See 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. 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.* at 216. 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). 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. *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 Section IV.B.3.a.v. 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 Section IV.B.3.a.vi. 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.).

VII.B. Forgery of Letters Patent—18 U.S.C. § 497

18 U.S.C. § 497 prohibits forging "letters patent" (described above), as well as knowingly passing off counterfeit letters patent:

> 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.

VII.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 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.

Congress prohibits false marking in part because a properly marked patented article provides the public with "a ready means of discerning the status of intellectual property embodied in an article of manufacture or design." *Bonito Boats, Inc. v. Adkins*, 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). 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).

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. Pacific Marine & Supply Co.*, 895 F.2d 761, 765 (Fed. Cir. 1990). Although not defined in the statute, courts have held that the phrase "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. Furthermore, "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 v. Sturm, Ruger & Co.*, 786 F.2d 1124, 1125 (Fed. Cir. 1986) (emphasis in original); *cf. Genlyte Thomas Group LLC v. National Servs. Indus.*, 262 F. Supp. 2d 753, 756 (W.D. Ky. 2003) (noting that courts consistently find no violation of § 292 "by a patentee who marks patented articles with more patents than actually cover the item") (internal citations and quotations omitted).

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 criminal offense. 35 U.S.C. § 292(a). Because it is a criminal fine for an infraction, 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).

Section 292(b) also provides for a civil *qui tam* remedy, which enables any person to sue for the statutory penalty and retain one-half of the recovery, leaving the other half "to the use of the United States." 35 U.S.C. § 292(b); *Boyd v. Schildkraudt 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.

Although criminal prosecutions pursuant to § 292 are rare, several reported private enforcement actions provide helpful authority for interpreting the false marking statute in criminal cases. 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).

By the same token, a defendant's "mere assertion" that he did not intend to deceive will not allow him to escape statutory liability when he knew of falsehood. *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"). "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." *Id.* at 1352 (citing *Seven Cases v. United States*, 239 U.S. 510, 517-18 (1916)). Using "objective standards," the prosecution may establish 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)). "Where 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.

VII.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

VIII.A. Introduction

This Chapter discusses the penalties for intellectual property crime, concentrating on the sentencing guidelines, restitution, and forfeiture.

This Chapter does not address the sentencing issues raised by former Attorney General John Ashcroft's September 23, 2003 *Memorandum on Department Policies and Procedures Concerning Charging Criminal Offenses, Disposition of Charges, and Sentencing*, *available at* http://www.usdoj.gov/opa/pr/2003/September/03_ag_516.htm, which instructs that "federal prosecutors must charge and pursue the most serious, readily provable offense or offenses that are supported by the facts of the case, except as authorized by an Assistant Attorney General, United States Attorney, or designated supervisory attorney in the limited circumstances described below." For more on charging decisions, prosecutors should consult the Attorney General's Memorandum, and also Chapter IX of this Manual, which specifically addresses charging decisions in intellectual property cases.

VIII.B. Statutory Penalties

The maximum statutory penalties for intellectual property crimes are addressed in the chapters on the respective substantive laws and are summarized in Appendix I.

VIII.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.

This Manual does not address the issues raised by *United States v. Booker*, 543 U.S. 220 (2005), in which the Supreme Court held that the United States Sentencing Guidelines must be considered at sentencing but are only advisory. As with other crimes, prosecutors should generally continue to seek sentences within the guidelines range in intellectual

property prosecutions because they are presumptively reasonable. Memorandum from Assistant Attorney General Christopher A. Wray, *Guidance Regarding the Application of United States v. Booker and United States v. Fanfan, 2005 WL 50108 (Jan. 12, 2005), to Pending Cases*, at 5 (Jan. 19, 2005). 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 Deputy Attorney General James B. Comey's January 28th, 2005 *Memorandum on Department Policies and Procedures Concerning Sentencing*, which directs that "federal prosecutors must actively seek sentences within the range established by the Sentencing Guidelines in all but extraordinary cases."

For assistance with any sentencing issues specific to intellectual property crimes, please call CCIPS at (202) 514-1026 for assistance.

VIII.C.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

VIII.C.1.a. Applicable Guideline is § 2B5.3

U.S.S.G. § 2B5.3 governs sentencing for the following offenses:

- Criminal copyright infringement, 17 U.S.C. § 506, 18 U.S.C. § 2319
- Criminal violations of the Digital Millennium Copyright Act, 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.

The one exception is the Digital Millennium Copyright Act, which is not listed in the guidelines' index at all. A statute not listed in this index should be sentenced under "the most analogous guideline." U.S.S.G. §§ 1B1.2(a), 2X5.1. In DMCA cases, the most analogous guideline is § 2B5.3. The DMCA was intended to safeguard the copyright protections for copyrighted works, and copyright crimes are sentenced under § 2B5.3. Moreover, § 2B5.3 implicitly refers to the DMCA in an application note that requires an adjustment for use of a special skill under U.S.S.G. § 3B1.3 "[i]f the defendant de-encrypted or otherwise circumvented a technological security measure to gain initial access to an infringed item." U.S.S.G. § 2B5.3 cmt. n.3 (2005). Although the DMCA and U.S.S.G. § 2B5.3 are not a perfect fit, they are the best match under the current guidelines.

Section 2B5.3 has been amended a number of times. It was amended on May 1, 2000, 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). Section 2B5.3 was amended again effective October 24, 2005, adding a new specific offense characteristic (2) addressing infringement of pre-release works, renumbering offense characteristics (2)-(4) as offense characteristics (3)-(5), clarifying the definition of uploading for technical purposes, and clarifying that the court can estimate the infringement amount using any relevant information. *See* U.S.S.G. App. C (Amendment 675).

As of this writing, U.S.S.G. § 2B5.3 is likely to be amended again during 2006 pursuant to the Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1, 120 Stat. 285, 287-88 (Mar. 16, 2006). It asks the Sentencing Commission to explore how the guideline should account for items that facilitate infringement such as counterfeit labels

and DMCA circumvention devices. See also Section III.E.5. of this Manual.

As is discussed in Section VIII.C.2. of this Chapter, the Economic Espionage Act is sentenced under U.S.S.G. § 2B1.1.

VIII.C.1.b. Base Offense Level

U.S.S.G. § 2B5.3's base offense level is currently 8, up from a base offense level of 6 for offenses committed before May 1, 2000. *See* U.S.S.G. App. C (Amendments 590, 593). The base offense level was raised from 6 to 8 to reflect that "the vast majority" of intellectual property offenses involve more than minimal planning. *Id.*

VIII.C.1.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 then 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.

VIII.C.1.c.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 a variety 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 VIII.C.1.c.iii. of this Chapter. The individual infringement amounts are then aggregated into a total infringement amount, which is then plugged into the loss table in U.S.S.G. § 2B1.1. See Section VIII.C.1.c.v. of this Chapter.

VIII.C.1.c.ii. Number of Infringing Items

The number of infringing items can 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. When the number of infringing items is difficult or impossible to calculate, however, reasonable estimates are allowed. See Section VIII.C.1.c.iv. of this Chapter.

In determining the number of infringing items, the biggest questions are often whether or to what extent to include items that are incomplete, such as items in the process of production, or that merely facilitate infringement, such as labels and packaging. These questions are discussed at length in Sections III.E.5. (sentencing issues concerning counterfeit marks) and VI.E.5. (sentencing issues concerning counterfeit and illicit labels, documentation, and packaging for copyrighted works) of this Manual. They are also likely to be addressed in upcoming guideline amendments that will be considered after this Manual is published mid-2006.

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. If trafficking is an element of the crime, then the infringement amount should include all items the defendant acquired because the intellectual property crimes define trafficking to include obtaining control over the infringing product with the intent to transport, transfer, or dispose of it. *See United States v. DeFreitas*, No. 98 CR. 1004(RWS), 2000 WL 763850, at *1 (S.D.N.Y. June 13, 2000) (trademark case), *aff'd on other grounds*, 8 Fed. Appx. 58 (2d Cir. 2001). The infringement amount should also include all the items the defendant acquired if he is convicted of an attempt, *id.*, or conspiracy. In such cases, the infringement amount should include all infringing items in the defendant's inventory, plus all infringing items that had been transferred out of inventory.

Determining the number of infringing items in a DMCA case can be a challenge because a defendant can violate the DMCA without engaging in any infringement. See Chapter V of this Manual. The guideline and its commentary give no help. Because these issues are complex and are also likely to be addressed in guidelines amendments that will be considered after this Manual is published in 2006, prosecutors are encouraged to consult CCIPS for guidance at (202) 514-1026.

VIII.C.1.c.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 Sections III.E.5. and VI.E.5. of this Manual.

- **Items that Facilitate Infringement Such as Labels and DMCA Circumvention Devices**

How to value items that do not infringe but instead enable infringement—such as counterfeit labels, packaging, and documentation, as well as DMCA-violating circumvention devices—raises complex issues. These issues include whether to use the value of the item that facilitates infringement (such as the label or circumvention device) or the item that would be infringed, and how to value items that could facilitate the infringement of a variety of items that have disparate prices (such as clothing labels that could be attached to low-priced children's clothing or high-priced men's suits or ladies' dresses). These issues are discussed briefly in Sections III.E.5. and VI.E.5. of this Manual, and are also likely to be addressed in upcoming guideline amendments that will be considered after this Manual is published in 2006.

- **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 counterfeits 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 or not. 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 was hard to determine, then the harm should be computed at the legitimate item's price for ease of calculation.

The guidelines, however, originally 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 presented some difficulties when the counterfeit items had been distributed for free, such as pirated software and music that was freely available over the Internet, which would have resulted 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: whereas the retail value of legitimate items is easily measured, the retail value of counterfeit items is not always obvious.

Notwithstanding the original guidelines' silence as to a legitimate item's retail value, the 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 United States v. Slater*, 348 F.3d 666, 670 (7th Cir. 2003) (refusing to assess zero value to free software distributed over the Internet because courts "need only make a reasonable estimate of the loss, given the available information"); *United States v. Bao*, 189 F.3d 860, 866-67 (9th Cir. 1999) (stating that the retail value of genuine merchandise is relevant as a ceiling for the retail value of infringing items); *United States v. Cho*, 136 F.3d 982, 985 (5th Cir. 1998) (stating that it is "not clear error for the district court to rely on the retail value of genuine items [to assess] the retail value of the [counterfeit]

items," particularly when it is difficult to calculate the counterfeits' price); *United States v. Kim*, 963 F.2d 65, 69 (5th Cir. 1992) (holding that evidence of genuine items' retail value was relevant to the retail value for the counterfeits in absence of other evidence of counterfeits' value); *United States v. DeFreitas*, No. 98 CR. 1004 (RWS), 2000 WL 763850, at *2 (S.D.N.Y. June 13, 2000). In fact, the *Slater, Bao*, *Kim* and *DeFreitas* courts ultimately relied on the retail price of the infringed (legitimate) goods, even though the former guideline's plain language referred only to the retail value of the infringing (counterfeit) merchandise.

On May 1, 2000, the sentencing 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. cmt. n.2(A)(i)(I)**

Differences in appearance and quality therefore matter if they could be ascertained by "a reasonably informed purchaser." An infringing item that could fool only an uninformed purchaser would be valued at the counterfeit retail value.

- **The infringing item is a digital or electronic reproduction, *id.* cmt. n.2(A)(i)(II)**

For digital or electronic reproductions, use the retail value of an authentic item regardless of whether they appear authentic to a reasonably informed purchaser or not. A counterfeit movie DVD with an obviously counterfeit label would be valued at the authentic item's retail value, even though nobody would be confused into mistaking the counterfeit for an authentic DVD. The Commission's theory is likely that a digital or electronic reproduction is a perfect substitute for the real thing, whether its outer trappings look legitimate or not. The guideline 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, *id.* cmt. n.2(A)(ii)**

Again, the Commission likely reasoned that counterfeits sold at less than 75% of the authentic item's retail price are unlikely to fool consumers, or that consumers who would pay less than 75% of the authentic retail price would be unlikely to pay full price even if given the chance to do so.

- **The counterfeit's retail value "is difficult or impossible to determine without unduly complicating or prolonging the sentencing proceeding," *id.* cmt. n.2(A)(iii)**

As is discussed in Section VIII.C.1.c.iv. of this Chapter, reasonable estimates of the counterfeit and authentic 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," *id.* cmt. n.2(A)(iv)**

Presumably this rule would also apply to the illegal interception of cable and satellite service under statutes other than 18 U.S.C. § 2511, such as 47 U.S.C. §§ 553(b)(2), 605 and 17 U.S.C. § 1204.

- **The retail value of the authentic good is a better approximation of the harm than the value of the counterfeit, *id.* cmt. n.2(A)(v); or**
- **"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," *id.* 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 VIII.C.1.d. of this Chapter. Both these provisions were added on October 24, 2005. U.S.S.G. App. C (Amendment 675).

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).

VIII.C.1.c.iv. Determining Amounts and Values—Reasonable Estimates Allowed

How to determine the infringing or infringed item's retail value? Any relevant source of information is appropriate. 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 goes for determining the number of infringing items: actual counts are preferable, but approximations are appropriate.

The courts allowed approximations of the infringement amount even before the guidelines did so explicitly. *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); *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); *United States v. Kim*, 963 F.2d 65, 69-70 (5th Cir. 1992) (analogizing to fraud guideline for principle that reasonable estimates are acceptable).

Now, however, U.S.S.G. § 2B5.3 explicitly states that reasonable estimates are acceptable. On October 24, 2005, Application Note 2(E) to U.S.S.G. § 2B5.3 clarified as follows:

> (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). The reference to financial records is likely an incorporation of the holding in *Foote*.

Although statistical precision is preferable, it is not necessary. For example, in a case that turned on whether the 3,947 infringing pieces of computer software on a server were functioning or nonfunctioning, the FBI tested 71 programs and found that 94% were functioning. *United States v. Rothberg*, No. 00 CR 85, 2002 WL 171963, at *4 (N.D. Ill. Feb. 4, 2002), *aff'd on other grounds*, 348 F.3d 666 (7th Cir. 2003). To calculate the total number of functioning programs, the court multiplied the percentage from the sample (94%) by the total number of programs (3,947). *Id.* The court acknowledged that "the selection of the 71 programs was not random," but found that the selection was nevertheless "a reasonable basis for determining an estimate." *Id.*

Whatever estimates the parties offer, however, the parties must explain how their estimate was calculated and why. In *Rothberg*, *supra*, the government first estimated the number of functioning programs based on a mathematical function it claimed derived from "information regarding [data] transmission error rates [the government] obtained from companies that maintain telephone lines." *Id.* at *3. The court rejected this estimate because the government had not explained how it "had derived the calculation or why it should be considered a reasonable basis for estimating the number of functioning programs." *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.*, *Slater*, *supra*; *United States v. Foote*, No. C.R.A. 00-20091-01-KHV, 2003 WL 22466158, at *6 (D. Kan. July 31, 2003) (estimating infringement amount from trademark counterfeiting by subtracting legitimate income from bank deposits, and further discounting by the percentage of sales attributable to non-infringing items), *aff'd*, 413 F.3d 1240, 1251-52 (10th Cir. 2005).

VIII.C.1.c.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 U.S. v. Cho*, 136 F.3d 982 (5th Cir. 1998); *see also* U.S.S.G. App. C (Amendments 590, 593) (discussing infringement amount as similar to loss and an approximation of harm). On this technical point, *United States v. Sung*, 51 F.3d 92, 95 (7th Cir. 1995) is technically 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 U.S. v. Powell*, 139 Fed. Appx. 545 (4th Cir. July 19, 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) (unpublished opinion).

VIII.C.1.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). Consequently, effective October 24, 2005, 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 "work 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.

VIII.C.1.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). (Before the October 24, 2005 amendments, this provision was numbered § 2B5.3(b)(2). *See* U.S.S.G. App. C (Amendment 675).) 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 in an openly shared file." U.S.S.G. § 2B5.3 cmt. n.1 (Oct. 24, 2005). Uploading does not include merely downloading or installing an infringing item on a hard drive on a defendant's personal computer, unless the defendant places the infringing item in an openly shared file. *Id.* (Before the October 24, 2005 amendments, "uploading" was defined in § 2B5.3's first and third application notes. The 2005 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. The amendment made no substantive change, however. *See* U.S.S.G. App. C (Amendment 675).)

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 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 unless they involved

importation or uploading). In the case of counterfeit trademarked goods, manufacturing should include not only producing the item, but also applying a counterfeit label to it, since an item does not become counterfeit until a counterfeit label is used in conjunction with it.

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.").

VIII.C.1.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) [before October 24, 2005: § 2B5.3(b)(3)]

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. (This characteristic was renumbered from § 2B5.3(b)(3) to 2B5.3(b)(4) in the October 24, 2005 amendments. *See* U.S.S.G. App. C (Amendments 590, 593, 675).)

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. 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).

For a complete discussion of what qualifies as conduct done for the purposes of commercial advantage or private financial gain, see Section

II.B.4. of this Manual (copyright). 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).

VIII.C.1.g. Offense Involving Risk of Serious Bodily Injury or Possession of a Dangerous Weapon Increases the Offense Level by 2—U.S.S.G. § 2B5.3(b)(5) [before October 24, 2005: § 2B5.3(b)(4)]

If the offense involved conscious or reckless risk of 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 13, then it must be increased to level 13. *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 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). The October 24, 2005 amendments renumbered this enhancement from U.S.S.G. § 2B5.3(b)(4) to § 2B5.3(b)(5). *Id.* (Amendment 675).

VIII.C.1.h. Decryption or Circumvention of Access Controls Increases 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 "*shall* apply" if the defendant decrypted or circumvented access controls. U.S.S.G. § 2B5.3 cmt. n.3 (emphasis added) (formerly n.4, before the Oct. 24, 2005 amendments, *see* U.S.S.G. App. C (Amendment 675)).

Because the note quoted above refers only to the circumvention of access controls, it is unclear whether the special skill enhancement must also apply 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 VIII.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.

VIII.C.1.i. Upward Adjustment for Harm to Copyright or Mark-Owner's Reputation, Connection with Organized Crime, or Other Unspecified Grounds

The fourth application note for § 2B5.3 (formerly application note 5, before the October 24, 2005 amendments) states that an upward departure may be warranted if the offense level determined under § 2B5.3 "substantially understates the seriousness of the offense," such as when the offense substantially harmed the victim's reputation in a way that is otherwise unaccounted for, including in calculating the infringement amount, and when the offense was in connection with or in furtherance of a national or international organized criminal enterprise. U.S.S.G. § 2B5.3 cmt. n.4; *id.* App. C (Amendments 590, 593).These two examples are not, however, exclusive.

VIII.C.1.j. 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").

VIII.C.1.k. 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 secret, 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 6th 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, 546.

VIII.C.2. Offenses Involving the Economic Espionage Act

VIII.C.2.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.

VIII.C.2.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).

VIII.C.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.

VIII.C.2.c.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).

VIII.C.2.c.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).

VIII.C.2.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 or destroyed or, if the fair market value is impractible to determine or inadequately measures the harm, the cost to the victim of replacing that property," n.3(C)(i)
- "The cost of repairs to damaged property," n.3(C)(ii)
- "The approximate number of victims multiplied by the average loss to each victim," n.3(C)(iii)
- "The reduction that resulted from the offense in the value of equity securities or other corporate assets," n.3(C)(iv)
- "More general factors, such as the scope and duration of the offense and revenues generated by similar operations," n.3(C)(v)
- "[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," n.3(B)

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. Wilson*, 900 F.2d 1350 (9th Cir. 1990), a mail fraud case, a research associate offered to sell financial and

research data from his employer, a biotechnology and pharmaceutical firm, to a competitor. The defendant argued that the documents were worth their fair market value: the $100,000 to $200,000 that the competitor said it would have paid for them—the competitor worked with law enforcement to set up a sting—or the $200,000 that the defendant had said that he would sell them for. *Id.* at 1356. The Ninth Circuit, however, noted its "refus[al] to require a strict market value approach in determining the value of stolen goods," because that approach "measures only the gain to the defendant while virtually ignoring the harm suffered by the victim." *Id.* (citations omitted). Although the court acknowledged that the buyer's and seller's prices were relevant, it held that the trial court was entitled to value the documents at the victim's research and development costs for the information contained in the documents, especially because those costs indicate the intended loss to the victim. *Id.* Those costs totaled $4 million, although the trial court generously reduced the total by 75 percent, to $1 million, to give the defendant the benefit of every doubt. *Id.* at 1355.

Similarly, in *United States v. Ameri*, 412 F.3d 893, 900 (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. 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 Communications, 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.

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). It may also be that the criminal cases are largely consistent with civil cases' tendency when there is evidence for more than

one measure to "award that amount which is most beneficial to the injured party." 1 Richard Raysman & Peter Brown, *Computer Law: Drafting and Negotiating Forms* § 6.03A (2005).

- 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. 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). 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 University Computing Co. v. Lykes-Youngstown Corp.*, 504 F.2d 518 (5th Cir. 1974); *Vermont Microsystems, Inc. v. Autodesk Inc.*, 138 F.3d 449, 452 (2d Cir. 1998). 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
- 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 (2005). 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). 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) (2004).

A number of civil cases determine trade secrets' market value by calculating 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. *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* Uniform Trade Secrets Act § 3(a) (1985) ("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."); *Vitro Corp. v. Hall Chem. Co.*, 292 F.2d 678, 683 (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 *Molex, Inc. v. Nolen*, 759 F.2d 474 (5th Cir. 1985); *University Computing Co.*, 504 F.2d 518; *Linkco, Inc. v. Fujitsu Ltd.*, 232 F. Supp. 2d 182, 186-87 (S.D.N.Y. 2002) (holding that a "reasonable royalty is the

best measure of damages in a case where the alleged thief made no profits"); *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
- 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; and
- the market price that the defendant actually received or paid in exchange for the technology

VIII.C.2.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 the offense to benefit a foreign government, foreign instrumentality, or foreign agent. *See* U.S.S.G. § 2B1.1(b)(5).

VIII.C.2.e. Sophisticated Means—U.S.S.G. § 2B1.1(b)(9)(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)(9)(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 often 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. 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); *United States v. Minneman*, 143 F.3d 274, 283 (7th Cir. 1998).

VIII.C.2.f. 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).

VIII.C.2.g. 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.

VIII.C.2.h. 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. *Cf. United States v. Straus*, 188 F.3d 520, 1999 WL 565502, at *5 (10th Cir. 1999) (table) (holding that abuse-of-trust and more-than-minimal-planning enhancements, the latter in a predecessor to U.S.S.G. § 2B1.1(b)(9)(C), can be applied to same conduct simultaneously).

VIII.C.2.i. 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 an 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).

"'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).

VIII.C.2.j. No Downward Departure for Victim's Participation in Developing the Case

As noted in Section VIII.C.1.k. of this Chapter, the court may not depart downward on the ground that the victim participated in the prosecution.

VIII.D. Restitution

"'The principle of restitution is an integral part of virtually every formal system of criminal justice, of every culture and every time. It holds that, whatever else the sanctioning power of society does to punish its wrongdoers, it should also ensure that the *wrongdoer is required to the degree possible to restore the victim to his or her prior state of well-*

being.'" *Attorney General Guidelines on Victim and Witness Assistance*, Art. V.A. (Dep't of Justice May 2005) (emphasis added in original) (quoting S. Rep. No. 104-179, at 12-13 (1996), *reprinted in* 1996 U.S.C.C.A.N. 924, 925-26).

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 in intellectual property crimes. For more detailed guidance on restitution principles and procedures, prosecutors should consult the *Attorney General Guidelines on Victim and Witness Assistance*, cited above, as well as the *Prosecutor's Guide to Criminal Monetary Penalties: Determination, Imposition and Enforcement of Restitution, Fines & Other Monetary Impositions* (Dep't of Justice Office of Legal Education May 2003).

VIII.D.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). 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 few cases on point confirm that intellectual property offenses are "offense[s] against property" for the purpose of § 3663A. *See United States v. Chay*, 281 F.3d 682 (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. B64-01, 2003 WL 22705133 (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, 1195 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 in all Title 18 intellectual property offenses, including § 1831 (economic espionage to benefit foreign government, instrumentality, or agent), § 1832 (general economic espionage), § 2318 (counterfeit and illicit labels and counterfeit documentation and packaging for copyrighted works), § 2319 (copyright), § 2319B (camcorded movies), and § 2320 (goods, services, labels, documentation, and packaging with counterfeit marks). In addition, Congress recently made clear that restitution must be ordered in appropriate § 2320 cases. *See* 18 U.S.C. § 2320(b)(4) (as amended by the Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, § 1, 120 Stat. 285, 286 (enacted March 16, 2006)).

This list might also include violations of § 2319A (bootleg music and music video recordings), but defendants might 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 II.F. of this Manual (describing § 2319A's constitutional basis as the Commerce Clause rather than the Intellectual Property Clause), 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.

There are two principal exceptions to mandatory restitution provided for 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 of retail counterfeit goods cases 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. 18 U.S.C. § 3664(d)(5); *U.S. v. Grimes*, 173 F.3d 634 (7th Cir. 1999)." *Prosecutor's Guide to Criminal Monetary Penalties: Determination, Imposition and Enforcement of Restitution, Fines & Other Monetary Impositions* 28 (Dep't of Justice Office of Legal Education May 2003). Department policy also requires that "[w]hen this exception does apply, the prosecutor should nevertheless *seek restitution for the benefit of the victims to the extent practicable*," *Attorney General Guidelines on Victim and Witness Assistance* Art. V.F. (Dep't of Justice May 2005) (emphasis added), such as by asking 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 how to set 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. See Section III.E.3. of this Manual. 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. *Id.*

Although technically not an exception to the mandatory restitution provisions in 18 U.S.C. § 3663A, there are two classes of intellectual property crimes for which there is no mandatory restitution under § 3663A. The first class consists of those intellectual property offenses

located outside Title 18 of the United States Code. Mandatory restitution applies only to an "offense against property under this title [18]," 18 U.S.C. § 3663A(c)(1)(A)(ii), which by definition excludes intellectual property offenses located outside Title 18. These include violations of the Digital Millennium Copyright Act, 17 U.S.C. § 1204, and the unauthorized reception of cable and satellite service as prohibited by 47 U.S.C. §§ 553(b)(2), 605.

The second class consists of any intellectual property offenses located in Title 18 that might be characterized as not being "offense[s] against *property*." § 3663A(c)(1)(A)(ii) (emphasis added). Examples might include violations of 18 U.S.C. § 2319A (bootleg music and music video recordings).

Fortunately, even in the cases discussed in the previous paragraphs, there are other mechanisms to obtain restitution. For intellectual property offenses that are located in Title 18 but are not offenses against property, discretionary restitution is available under 18 U.S.C. § 3663(a)(1)(A). For intellectual property offenses that are located outside Title 18, restitution is available under a plea agreement. *See* 18 U.S.C. § 3663(a)(3). And, finally, discretionary restitution can be ordered for *any* intellectual property crime—in fact any crime at all, whether an intellectual property crime or not, whether in Title 18 or not, and whether an offense against property or not—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) (unpublished), 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.

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.

In deciding whether to order 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 Attorney General Guidelines on Victim and Witness Assistance* Arts. V.C.1. (stating that "[w]hen exercising their discretion, prosecutors shall give due consideration to the need to provide full restitution to the victims of Federal criminal offenses," among other charging considerations), V.D.1.-.6. (plea agreements, including required provisions and supervisors' duties for approval relating to restitution). 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.*

VIII.D.2. Victims Include Owners of Intellectual Property and Consumers Who Were Defrauded

Prosecutors should consider all victims who suffered a loss, from the holder of the intellectual property to the direct purchaser and the 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 VIII.D.1. of this Chapter, DMCA offenses do not qualify for mandatory restitution. Moreover, the cases suggest that in DMCA or DMCA-like cases, the company whose technological measures are circumvented is not entitled to restitution unless the company also owns copyrighted works that were infringed as a result of the circumvention. *See 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]."); *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.

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: Determination, Imposition and Enforcement of Restitution, Fines & Other Monetary Impositions* 32 (Dep't of Justice Office of Legal Education May 2003), 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, 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). Where the offense of conviction includes a scheme, conspiracy, or pattern of criminal activity, however, restitution can be imposed for the entire scheme, conspiracy, or pattern. 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 cannot be tied together with a scheme, pattern, or conspiracy, then the acts outside the offense of conviction generally do not trigger restitution. 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—for example, if the offense of conviction is *possession* of stolen credit cards, some courts will not impose restitution for the victims of the *use* of the cards. *See, e.g., United States v. Blake*, 81 F.3d 498 (4th Cir. 1996); *United States v. Hayes*, 32 F.3d 171 (5th Cir. 1994). However, some courts apply this rule more strictly than others. For example, to determine the existence of a scheme and what acts it included, 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. Jackson*, 155 F.3d 942 (8th Cir. 1998); *United States v. Ramirez*, 196 F.3d 895 (8th Cir. 1999); *United States v. Hughey (II)*, 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 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: Determination, Imposition and Enforcement of Restitution, Fines & Other Monetary Impositions* 22-24 (Dep't of Justice Office of Legal Education May 2003).

At the beginning of the case, prosecutors should draft the indictment to maximize restitution. *Id.* at 21. As the Executive Office for United States Attorneys 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.

VIII.D.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 cf. 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. 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 is entitled to no restitution. *See 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 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. 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 $500-$100,000 (up to $1 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 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), *cert. denied*, 126 S. Ct. 1382 (2006); *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, 783 (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).

Third, 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* 18 U.S.C. § 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.* Department policy requires full restitution in discretionary cases (assuming the defendant's current or future economic circumstances warrant it), unless economic circumstances warrant nominal payment. *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); *Attorney General Guidelines for Victim and Witness Assistance* Art. IV.B.2.b(4) (May 4, 2005). 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(d). 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.

VIII.E. Forfeiture

In intellectual property (IP) crimes, 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 IP crimes prevents their being used to commit further IP crime. Forfeiting the proceeds of IP crime—the revenues and profits—prevents their reinvestment in a criminal enterprise. Finally, forfeiture can serve as a powerful deterrent.

Congress has passed many forfeiture laws that address specific crimes, but in a manner that has created a complex web of forfeiture statutes. The specific IP forfeiture provisions vary with the IP crime, yet the underlying criminal IP statute will often not make it obvious which forfeiture remedies—administrative, civil, or criminal—are available.

To make IP forfeiture more standard and intuitive, Congress passed the Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, 120 Stat. 285 (enacted March 16, 2006) to expand the type of property that can be forfeited and to clarify and standardize the procedures for doing so. The Act, however, affects only counterfeit trademark, service mark, and certification mark offenses in 18 U.S.C. § 2320. Consequently, the Administration has proposed similar amendments to the forfeiture provisions for other IP offenses.

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. Due to the intricacies of forfeiture law (including both recent changes in 2006 and possible future revisions), 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.

VIII.E.1. Property Subject to Forfeiture

Intellectual property crimes give rise to three general categories of forfeitable property:

- 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). These items are generally subject to forfeiture.

- Proceeds derived from the commission of an IP offense. These are also usually forfeitable.
- 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. Forfeiture of facilitating property is available in many cases, but its availability varies substantially depending on the specific IP offense, the type of property, and the type of forfeiture sought.

VIII.E.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.

VIII.E.2.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.

Administrative forfeiture in IP offenses is usually limited to situations that implicate the customs laws. For example, Immigration and Customs Enforcement (ICE) may seize, forfeit, and destroy imported copyright-infringing products administratively pursuant to 17 U.S.C. §§ 509(b) and 603(c). ICE may also seize, forfeit, and destroy imported trademark-infringing products administratively under 19 U.S.C. § 1526(e). Administrative forfeiture may also be available for violations of 18 U.S.C. §§ 2318 and 2319A. *See* 18 U.S.C. § 2318(e); 17 U.S.C. § 509; *see also* 18 U.S.C. § 981(d); 19 U.S.C. §§ 1607-09 (administrative forfeiture of proceeds); 49 U.S.C. § 80304 (administrative forfeiture of 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.

VIII.E.2.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 is executed as part of a criminal 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.

VIII.E.2.c. Table of Forfeiture Provisions Arranged by Criminal IP Statute

The following list indicates the types of forfeiture available for each intellectual property offense. 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 is not provided for directly, it may be available indirectly through money laundering statutes.

CRIMINAL COPYRIGHT INFRINGEMENT

Administrative	**Yes.** 17 U.S.C. §§ 509(a) (forfeiture of infringing goods) and (b) (applying customs laws), 602-603 (specifically prohibiting imports of infringing copies). 18 U.S.C. § 981(d) (allowing administrative forfeiture for proceeds

	forfeitable civilly); 19 U.S.C. §§ 1595a, 1607-09.
Civil	
Infringing Items	**Yes**. 17 U.S.C. §§ 509(a), 602-603 (prohibiting imports).
Facilitating Property	**Yes.** 17 U.S.C. § 509(a) (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.** 17 U.S.C. §§ 506(b), 602-603; 28 U.S.C. § 2461(c) (allowing criminal forfeiture where property could be seized civilly).
Facilitating Property	**Yes**. 17 U.S.C. § 506(b); 28 U.S.C. § 2461.
Proceeds	**Yes.** 18 U.S.C. § 981(a)(1)(C); 28 U.S.C. § 2461(c).

DIGITAL MILLENNIUM COPYRIGHT ACT

Administrative	**No.**
Civil	**None.**
Criminal	**None.**

ECONOMIC ESPIONAGE ACT (TRADE SECRET THEFT)

Administrative	**No.**
Civil	**None.**
Criminal	
Facilitating Property	**Yes (discretionary)**. 18 U.S.C. § 1834(a)(2).
Proceeds	**Yes (mandatory).** 18 U.S.C. § 1834(a)(1).

COUNTERFEIT/ILLICIT LABELS, DOCUMENTATION, AND PACKAGING FOR COPYRIGHTED WORKS

Administrative	**Yes.** 18 U.S.C. § 2318(e); 17 U.S.C. § 509(b); 18 U.S.C. § 981(d); 19 U.S.C. §§ 1595a (allowing seizure and forfeiture by Customs), 1607-09.
Civil	
Counterfeit/ Infringing Items	**Yes.** 18 U.S.C. § 2318(e); 17 U.S.C. § 509.
Facilitating Property	**Yes.** 18 U.S.C. § 2318(e); 17 U.S.C. § 509.
Proceeds	**Yes.** 18 U.S.C. §§ 981(a)(1)(C), 1956(c)(7).
Criminal	
Counterfeit/ Infringing Items	**Yes (mandatory).** 18 U.S.C. § 2318(d).
Facilitating Property	**Yes (mandatory as to plates, molds, masters, etc.; discretionary as to other equipment).** 18 U.S.C. § 2318(d).
Proceeds	**Yes.** 18 U.S.C. §§ 981(a)(1)(C), 1956(c)(7); 28 U.S.C. § 2461(c).

UNAUTHORIZED FIXATIONS OF LIVE MUSICAL PERFORMANCES ("BOOTLEGGING")

Administrative	**Yes.** 18 U.S.C §§ 2319A(c), 981(d); 19 U.S.C. §§ 1595a, 1607-09.
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).
Facilitating Property	**Yes (mandatory for plates, molds, masters, etc.; discretionary as to other equipment).** 18 U.S.C. § 2319A(b).
Proceeds	**Yes.** 18 U.S.C. §§ 981(a)(1)(C), 1956(c)(7); 28 U.S.C. § 2461(c).

UNAUTHORIZED RECORDING OF MOTION PICTURES ("CAMCORDING")

Administrative	**No.**
Civil	**None.**
Criminal	
Unauthorized Recordings	**Yes (mandatory).** 18 U.S.C. § 2319B(b).
Facilitating Property	**Yes (mandatory).** 18 U.S.C. § 2319B(b).
Proceeds	**No.**

GOODS, SERVICES, LABELS, DOCUMENTATION, AND PACKAGING WITH COUNTERFEIT MARKS

***NOTE: 18 U.S.C. § 2320(b) was amended on March 16, 2006. The table below reflects these amendments. The pre-amendment provision is discussed and quoted in Sections VIII.E.4.b. and VIII.E.5. of this Chapter.

Administrative	**Yes.** 19 U.S.C. §§ 1595a, 1607-09; 18 U.S.C. § 981(d);
Civil	
Counterfeit Items	**Yes.** 18 U.S.C. § 2320(b)(1)(A).
Facilitating Property	**Yes.** 18 U.S.C. § 2320(b)(1)(B).
Proceeds	**Yes.** 18 U.S.C. §§ 981(a)(1)(C); 1956(c)(7); 28 U.S.C. § 2461(c).

Criminal

Counterfeit Items	**Yes (mandatory).** 18 U.S.C. § 2320(b)(3)(A).
Facilitating Property	**Yes (mandatory).** 18 U.S.C. § 2320(b)(3)(A).
Proceeds	**Yes.** 18 U.S.C. § 2320(b)(3)(A); *or alternatively:* 18 U.S.C. §§ 981(a)(1)(C), 1956(c)(7); 28 U.S.C. § 2461(c).

VIII.E.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. 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, as it can dispose of certain forfeiture matters quickly in a non-judicial setting.

VIII.E.4. Civil Forfeiture in IP Matters

Civil forfeiture is available in some (though not all) intellectual property offenses. It is available for property connected to criminal copyright infringement, 18 U.S.C. § 2319; trafficking in counterfeit or illicit labels or counterfeit documentation or packaging for copyrighted works, 18 U.S.C. § 2318; unauthorized fixations of live musical performances, 18 U.S.C. § 2319A; and trafficking in goods, services, labels, documentation, or packaging with counterfeit marks, 18 U.S.C. § 2320. Civil forfeiture is not available if the property is only connected to violations of the Digital Millennium Copyright Act, 17 U.S.C. § 1204, or the Economic Espionage Act, 18 U.S.C. §§ 1831, 1832. Again, the government need only prove that the crime was committed; it need not convict a specific defendant of the crime.

VIII.E.4.a. Proceeds

The government can forfeit the proceeds of 18 U.S.C. §§ 2318, 2319, 2319A, and 2320 offenses in civil forfeiture proceedings. Under the Civil Asset Forfeiture Reform Act of 2000 ("CAFRA") amendments to 18 U.S.C. § 981(a)(1)(C), a general civil forfeiture statute, the government can 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). 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). Thus, civil forfeiture of proceeds is available for violations of 18 U.S.C. §§ 2318, 2319, 2319A, and 2320.

VIII.E.4.b. Infringing Items, Other Contraband, and Facilitating Property

Civil forfeiture of infringing and other contraband items, as well as facilitating property, is also available for some IP offenses, but varies greatly depending on the particular offense and property involved.

For some copyright and copyright-related offenses, Title 17 provides for civil forfeiture of contraband such as infringing copies and certain types of facilitating property. Civil forfeiture is available against property that was manufactured or used in violation of the copyright laws, 17 U.S.C. § 509(a), specifically (a) infringing copies, or copies intended for infringing use; and (b) the plates, masters, or other means used for reproducing the infringing copies, as well as other devices for manufacturing, reproducing, or assembling infringing copies. *See, e.g., United States v. One Sharp Photocopier, Model SF-7750*, 771 F. Supp. 980, 983 (D. Minn. 1991) (holding that the government was entitled to forfeiture of copier used to produce infringing copies of a software instruction manual); *see also* 17 U.S.C. § 509(b) (incorporating administrative forfeiture provisions of Title 19 and the provisions relating to *in rem* admiralty actions). Civil forfeiture is also available against infringing articles or unauthorized fixations imported into the United States, in some circumstances. *See* 17 U.S.C. §§ 602-603 (infringing copies); 18 U.S.C. § 2319A (unauthorized fixations of live musical performances).

For counterfeit trademark, service mark, and certification mark offenses, the forfeiture provisions changed markedly in 2006. Before the March 16, 2006 amendments, there was no civil forfeiture authority for these cases except in the context of importation or proceeds under the specified unlawful activity provisions discussed in above. However, the old version of the statute, 18 U.S.C. § 2320, included a hybrid forfeiture provision that used the civil preponderance-of-the-evidence standard but applied only in a criminal prosecution. Before its amendment, § 2320(b) provided that "[u]pon a determination by a preponderance of the evidence that any articles in the possession of a defendant in a prosecution under this section bear counterfeit marks, the United States may obtain an order for the destruction of such articles." 18 U.S.C. § 2320(b) (West 2005). Congress enacted this provision because "[e]ven if the defendant is ultimately acquitted of the criminal charge, there is no valid public policy reason to allow the defendant to

retain materials that are in fact counterfeit." *Joint Statement on Trademark Counterfeiting Legislation*, 130 Cong. Rec. 31,674 (1984). *See also United States v. Foote*, 238 F. Supp. 2d 1271 (D. Kan. 2002). This provision was revised considerably, however, by the Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, 120 Stat. 285 (enacted March 16, 2006) to provide for civil forfeiture of "[a]ny article bearing or consisting of a counterfeit mark used in committing" a § 2320 violation, and "[a]ny property used, in any manner or part, to commit or to facilitate the commission of" such a violation. 18 U.S.C. § 2320(b)(1).

VIII.E.4.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.

VIII.E.4.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(f).

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.

VIII.E.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).

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.

Criminal forfeiture is available for at least some types of property in cases involving the following criminal IP statutes: copyright, 17 U.S.C. § 506, 18 U.S.C. § 2319; trade secret theft, 18 U.S.C. § 1834;

trafficking in counterfeit or illicit labels or counterfeit documentation or packaging for copyrighted works, 18 U.S.C. § 2318; trafficking in goods, services, labels, documentation, or packaging with counterfeit marks, 18 U.S.C. § 2320; bootlegged recordings of live musical performances, 18 U.S.C. § 2319A; and movie camcording, 18 U.S.C. § 2319B. Currently, there are no criminal forfeiture provisions for violations of the Digital Millennium Copyright Act, 17 U.S.C. § 1204.

VIII.E.5.a. Proceeds

The government can obtain criminal forfeiture of IP crime proceeds whenever those proceeds could be forfeited civilly: 18 U.S.C. §§ 2318, 2319, 2319A, and 2320. This is because CAFRA generally provided that criminal forfeiture is available whenever civil forfeiture is available:

> If a person is charged in a criminal case with a violation of an Act of Congress for which the civil or criminal forfeiture of property is authorized, the Government may include notice of the forfeiture in the indictment or information pursuant to the Federal Rules of Criminal Procedure. If the defendant is convicted of the offense giving rise to the forfeiture, the court shall order the forfeiture of the property as part of the sentence in the criminal case pursuant to the Federal Rules of Criminal Procedure and section 3554 of title 18, United States Code. The procedures in section 413 of the Controlled Substances Act (21 U.S.C. § 853) apply to all stages of a criminal forfeiture proceeding, except that subsection (d) of such section applies only in cases in which the defendant is convicted of a violation of such Act.

28 U.S.C. § 2461(c). As discussed above, the offenses for which civil forfeiture is available are enumerated in 18 U.S.C. § 981, and include any offense constituting "specified unlawful activity" under 18 U.S.C. § 1956(c)(7), the money laundering statute. Section 1956(c)(7)'s list of "specified unlawful activity" includes, directly or indirectly, violations of 18 U.S.C. §§ 2318, 2319, 2319A, and 2320.

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 § 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).

In addition, for counterfeit marks cases, the Stop Counterfeiting in Manufactured Goods Act (enacted March 16, 2006, discussed in Section VIII.E.4. of this Chapter) amended 18 U.S.C. § 2320 to provide for mandatory criminal forfeiture of proceeds (as well as other property). *See* 18 U.S.C. § 2320(b)(3)(A)(i) (as amended Mar. 16, 2006).

The Economic Espionage Act provides for mandatory criminal forfeiture of the proceeds of a violation of 18 U.S.C. § 1831 or § 1832. *See* 18 U.S.C. § 1834(a)(1).

VIII.E.5.b. Infringing Items, Other Contraband, and Facilitating Property

Generally, criminal forfeiture is available against contraband items involved in an IP offense—such as infringing items, unauthorized recordings, and counterfeit labels or marks or articles bearing such marks—and in some cases those items are subject to mandatory destruction. Facilitating property is likewise subject to criminal forfeiture in most cases, although such equipment generally need not be destroyed and can instead be disposed of in other ways, such as at auction.

Copyright offenses are subject to mandatory forfeiture: "When any person is convicted of a violation of subsection (a), the court in its judgment of conviction shall, in addition to the penalty therein prescribed, order the forfeiture and destruction or other disposition of all infringing copies or phonorecords and all implements, devices, or equipment used in the manufacture of such infringing copies or phonorecords." 17 U.S.C. § 506(b).

Criminal forfeiture is likewise mandatory in offenses for camcording and trafficking in counterfeit and illicit labels and counterfeit documentation and packaging for copyrighted works. *See* 18 U.S.C. § 2318(d) (stating that the court must order "the forfeiture and destruction or other disposition of all counterfeit labels or illicit labels and all articles to which counterfeit labels or illicit labels have been affixed or which were intended to have had such labels affixed, and of any equipment, device, or material used to manufacture, reproduce, or assemble the counterfeit labels or illicit labels"); 18 U.S.C. § 2319B(b) (stating that upon conviction, the court "shall, in addition to any penalty provided, order the forfeiture and destruction or other disposition of all unauthorized copies of motion pictures or other audiovisual works

protected under title 17, or parts thereof, and any audiovisual recording devices or other equipment used in connection with the offense").

The "bootleg" statute, 18 U.S.C. § 2319A(b), contains a similar forfeiture provision, requiring forfeiture and destruction of unauthorized recordings. However, unlike the mandatory forfeiture of equipment discussed above, the forfeiture of equipment used to reproduce unauthorized recordings of live musical performances is left to the discretion of the court, "taking into account the nature, scope, and proportionality of the use of the equipment in the offense." *Compare* 18 U.S.C. § 2319A(b) *with* 17 U.S.C. § 506(b).

For counterfeit marks cases, as noted above, until March 16, 2006, the criminal statute contained an unusual criminal forfeiture provision that allowed forfeiture of counterfeit goods upon a showing by a preponderance of the evidence (within or related to a criminal case) that the items bore counterfeit marks. *See* 18 U.S.C. § 2320(b) (West 2005). *See supra* II.E.4. Under the recent revisions to the forfeiture provisions in the Stop Counterfeiting in Manufactured Goods Act, 18 U.S.C. § 2320 now provides for mandatory forfeiture of "any article that bears or consists of a counterfeit mark used in committing the offense" and any of the defendant's property "used, or intended to be used, in any manner or part, to commit, facilitate, aid, or abet the commission of the offense." 18 U.S.C. § 2320(b)(3)(A). Any seized article bearing or consisting of a counterfeit mark must be destroyed. 18 U.S.C. § 2320(b)(3)(B).

The Economic Espionage Act, governing theft of trade secrets, provides for forfeiture of property used in facilitating the commission of the offense, considering the nature, scope, and proportionality of the use of the property in the offense. 18 U.S.C. § 1834(a)(2).

IX. Charging Decisions

IX.A. Introduction

In determining whether to charge an intellectual property crime, federal prosecutors should generally weigh the same considerations 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; and 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, which includes:
  - 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.

IX.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.

IX.B.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 reportedly costs American companies $250 billion a year. U.S. Department of Justice, *Report of the Department of Justice's Task Force on Intellectual Property* 8 (Oct. 2004) (citing Office of the United States Trade Representative). As a consequence, "the American economy is losing hundreds of millions of dollars in tax revenues, wages, investment dollars, as well as hundreds of thousands of jobs." *Id.* The Justice Department has therefore made the enforcement of intellectual property laws a high priority. *Id.* at 13.

To meet this priority, 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. *See id.* at 13.

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. CCIPS can help evaluate whether a particular intellectual property crime poses a matter of federal priority. CCIPS can be reached at (202) 514-1026.

IX.B.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, the volume of infringement, the amount of revenue and profit, the number of participants, the involvement of organized crime, and the magnitude of the victim's loss or potential loss, all of which are factored into the sentencing guidelines. *See U.S. Sentencing Guidelines Manual* § 2B5.3(b)(1) & cmt. n.2(A) (2005) (volume of infringement and likelihood that defendant's sales displaced the victim's); *id.* cmt. 4(A)

(substantial harm to victim's reputation); *id.* app. note 4(B) (involvement of organized crime).

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**. Federal prosecutors should, however, 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 IX.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).
- **Counterfeit goods or services that endanger the public's health or safety deserve the highest consideration for prosecution.** *See* United States Department of Justice, *Report of the Department of Justice's Task Force on Intellectual Property* 7-9 (Oct. 2004); *cf.* U.S.S.G. § 2B5.3(b)(5) (adjusting offense level for

infringement offenses involving "conscious or reckless risk of serious bodily injury or possession of a dangerous weapon in connection with the offense" by 2 levels, with a minimum offense level of 13).

IX.B.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.

IX.B.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 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.

IX.B.5. The Individual's Willingness to Cooperate in the Investigation or Prosecution of Others

As discussed in Section IX.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.

IX.C. Whether the Person is Subject to Prosecution in Another Jurisdiction

The second 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 or local authorities. USAM 9-27.240 (comment). State or local law enforcement may be a viable alternative to federal prosecution. Federal intellectual property laws generally do not preempt state and local intellectual property laws. 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 traffic in some pirated works. *Compare* 17 U.S.C. § 301 (copyright preemption), *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), *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), *and 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), *with Anderson v. Nidorf*, 26 F.3d 100, 102 (9th Cir. 1994) (holding California anti-piracy statute not preempted by federal copyright laws in illegal sound recording case), *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).

IX.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. 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 infringing merchandise can also be subject to civil forfeiture and fines by United States Customs and Border Protection. *See, e.g.,* 19 U.S.C. § 1526(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.

IX.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 Criminal Resource Manual 162, *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00162.htm (also known as the "Thompson memo"). This memorandum's analysis applies to intellectual property crimes in the same manner as to other crimes.

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 and other high-tech 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 corporate rights-holders are often the primary victims in intellectual property offenses, consumers are victimized also. Some consumers may be defrauded into mistakenly buying counterfeits, while consumers who purchase authentic goods pay higher prices.

X.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 prosecutions. 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). Guidance for the implementation of the Justice for All Act can be found in the revised *Attorney General Guidelines for Victim and Witness Assistance* (May 2005) ("*AG Guidelines*"), which supersedes all earlier versions, and can be found at http://www.usdoj.gov/olp/final.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*, Art. I.B. 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. I.C.

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 and ultimately a petition for writ of mandamus in the Court of Appeals. *See* 18 U.S.C. § 3771(d)(3); *AG Guidelines*, Art. II.D.1. 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. I.D.2.; 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. II.D.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. II.D.1. In contrast, a "person whose injuries stem *only indirectly* from an offense is

not entitled to the rights or services described" above. *AG Guidelines*, Art. II.E.2 (emphasis added). Accordingly, 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 pursuant to 18 U.S.C.§ 3771(e), particularly in cases where there are hundreds or even thousands of potential victims.

The Act's provision on "Multiple Crime Victims" is of particular interest in cases involving the large-scale distribution of pirated digital works over the Internet:

> 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*, Art. II.G. For instance, in an online software piracy prosecution with hundreds or thousands of victims, it is often impractical for a prosecutor to notify all of the rights-holders. In such cases, the prosecutor should consider, at a minimum, notifying and enlisting the assistance of any trade organizations that represent multiple rights-holders. The prosecutor could then craft an alternative procedure for informing such representatives (in lieu of notifying all rights-holders) and move the court to approve it.

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(d).

X.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.

X.B.1. Reporting an Intellectual Property Crime

The Department recommends that victims of intellectual property crimes document all investigative steps, preserve evidence, and contact law enforcement right away. *See U.S. Department of Justice Report of the Department of Justice's Task Force on Intellectual Property* App. C (Oct. 2004). Victims can report intellectual property crimes using the referral forms in this Manual at Appendix H.

X.B.2. Ethical Concerns When the Criminal Prosecution Results in an Advantage in a Civil Matter

Like other victims of crime, IP rights-holders are often interested in securing economic and other relief, but, unlike many other victims, rights-holders often have the resources to aggressively pursue that relief themselves. 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. How concerned should the government be about IP victims using the threat of criminal prosecution to advance their private interests? And to what extent can the government 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?

X.B.2.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 a lawyer can ethically threaten to press criminal charges to advance a civil cause of action is not clear. The lack of clarity stems in part from a patchwork of ethical rules. The ABA's Model Code of Professional Responsibility (1969, amended 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." Disciplinary Rule 7-105(A). The ABA's Model Rules of Professional Conduct, adopted in 1983, omitted the rule as "redundant or overbroad or both." *See* ABA Formal Ethics Opinion 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* Disciplinary Rule 7-105(A) (Or. 2003) (allowing such threats "if, but only if, 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 prosecuting 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.

X.B.2.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.

U.S. Department of Justice, *Federal Grand Jury Practice* § 12.16 (Office of Legal Education 2000) (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 X.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 Section VIII.D.3. of this Manual (discussing 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(a)(5), 3664(f)(4). Therefore, it is perfectly appropriate for the government to require full restitution as a condition of a plea agreement. See Sections VIII.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 Professional Conduct R. 4.4 (2003).

Finally, there is the strategic concern. 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 X.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.

X.B.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.

Securities & 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 U.S. Department of Justice, *Federal Grand Jury Practice* ch. 12 (Office of Legal Education 2000). The following is a brief summary.

X.B.3.a. Private Civil Remedies

Victims of IP crimes have extraordinary enforcement mechanisms and civil 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(f) (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(f)(2)(A), (B) (illicit labels and counterfeit labels, documentation, and packaging for copyrighted works).

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 (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 (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 Section IX.D. of this Manual.

X.B.3.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 X.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 (1976) (adverse inference from silence permissible in prison disciplinary proceedings); *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 will conclusively establish 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.

X.B.3.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); *Securities & 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* U.S. Department of Justice, *Federal Grand Jury Practice* § 12.14, at 407-10 (Office of Legal Education 2000).

In 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 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).

X.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. This prompted the Department of Justice's Task Force on Intellectual Property to recommend that the Department issue guidance on the acceptance of resources from victims, related parties, and third parties. Accordingly, Deputy Attorney General Paul J. McNulty issued a memorandum to all United States Attorneys and Component Heads entitled "Guidance for Acceptance of Assistance and Gifts from Private Parties for Use in Connection with Investigations and Litigation" (May 2006). This subsection tracks the Deputy Attorney General's memorandum closely and highlights some of the issues addressed therein. 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 specific 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. The 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. The second issue 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. The third issue 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.

X.C.1. Gift Issues

X.C.1.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 Order 2400.2, *available at* http://www.usdoj.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 component. *Id.* ¶ 3.b.(1). Before accepting any gift, the AAG/A must consider: (1) whether the gift is appropriate for use; (2) whether the conditions the donor has placed on acceptance or use, if any, are "acceptable;" (3) whether 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 Assistant 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.

X.C.1.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.

X.C.1.b.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:

II. Providing factual or expert information in an investigation or fact or expert testimony at trial

IV. Turning over the fruits of an internal investigation (e.g., collecting and analyzing financial or transactional data)

VI. Consulting with law enforcement during the investigation (e.g., reviewing seized evidence to distinguish legitimate copyrighted works from forgeries, identifying proprietary information in a theft of trade secrets prosecution, or instructing professional staff and contractors to respond to queries from Departmental employees regarding technical subjects)

VIII. 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

X. 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.

X.C.1.b.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.

X.C.1.b.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 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.

X.C.1.b.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) and 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 during the pendency of the Department's case. 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 acceptance of 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.

X.C.1.b.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 its 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 not related 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 FBI and DEA 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.

X.C.1.b.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 specific 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.

X.C.1.c. Departmental Procedures for the Solicitation and Acceptance of Gifts and Assistance

X.C.1.c.i. Consultative Process for Acceptance of Assistance and Gifts

A law enforcement officer or Departmental 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 Deputy Designated Agency Ethics Official (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.

X.C.1.c.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.

X.C.1.c.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 Departmental Ethics Office, Justice Management Division, 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 Departmental Ethics Office, Justice Management Division.

X.C.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, 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 will be held 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).

X.C.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 4th 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) (holding that likelihood of influence on a prosecutor's charging decisions is reduced when the resources are devoted to investigating industry-related 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 (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. C97-1448 MJJ, 2001 WL 940904 (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.

X.C.4. Help and Advice

Each component (including each United States Attorney's Office) has qualified specialists to provide guidance, including a Deputy Designated Agency Ethics Official 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) 514-4024. 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 should first consult his or her supervisor and office Professional Responsibility Officer (PRO), who may then seek advice from the Professional Responsibility Advisory Office, telephone number (202) 514-3365.

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, or attempted to traffic, in [goods] [services]

   [offenses committed on or after March 16, 2006, can include labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature]

2. That such trafficking, or attempt to traffic, was intentional;

3. That the defendant

   [knowingly used a counterfeit mark on or in connection with the [goods] [services]]

   [offenses on or after March 16, 2006, can also include: knew that counterfeit marks had been applied to the labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging]

   in which the defendant trafficked, or attempted to traffic; and

4. That the use of the counterfeit marks 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 for those goods or services 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"

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)

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)

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 infringed EITHER

   (a) for purposes of commercial advantage or private financial gain,(17 U.S.C.§ 506(a)(1)(A)(numbered § 506(a)(1) by the Apr. 27, 2005 amendments) & 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 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

Section 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)

Section 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)

Section 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

Section II.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

Section II.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)

17 U.S.C. §§ 1201(a)(1)(A), 1204(a)

Section V.B.

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

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

Commercial Theft of Trade Secrets

18 U.S.C. § 1832

Chapter IV

Elements

1. The defendant misappropriated a trade secret from its owner
2. The defendant knew or had a firm belief that the item/information was a trade secret
3. The item/information was in fact a trade secret (except in cases of attempt or conspiracy)
4. The defendant intended to convert the trade secret to the economic benefit of anyone other than the owner
5. The defendant intended or knew the theft would injure the owner of the trade secret
6. The trade secret was related to or was included in a product that was produced for or placed in interstate or foreign commerce

Defenses

Parallel development: Others may discover information underlying a trade secret through their own independent efforts.

Reverse engineering: Others may discover 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

Foreign Economic Espionage

18 U.S.C. § 1831

Chapter IV

Elements

1. The defendant misappropriated a trade secret from its owner
2. The defendant knew or had a firm belief that the item/information was a trade secret
3. The item/information was in fact a trade secret (except in cases of attempt or conspiracy)
4. The defendant intended or knew the theft would benefit any foreign government, foreign instrumentality or foreign agent

Defenses: See **Commercial Theft of Trade Secrets** (18 U.S.C. § 1832).

Pre-Indictment Approval Required

Statutory maximum penalty: 15 years' imprisonment and fine of $500,000 or twice the gain/loss (individual); $10,000,000 fine 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)

Section IV.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 if the conduct involved an interstate or foreign communication ....

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 (second offense)

Guideline section: United States Sentencing Guideline § 2B1.1

Appendices B-F

Sample Indictments and Jury Instructions

Sample indictments and jury instructions for these offenses are available on DOJNET at http://10.173.2.12/usao/eousa/ole/usabook/ipma/appx.htm.

Appendix G

Intellectual Property Contact List

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

http://www.usdoj.gov

Prosecution of, and guidance, support, resources, and materials for prosecuting domestic and international criminal intellectual property offenses; development of intellectual property enforcement policy; and support and oversight of the federal prosecution of intellectual property crimes.

National Intellectual Property Rights Coordination Center

U.S. Immigration and Customs Enforcement (ICE)

1300 Pennsylvania Avenue NW, Room 3.5A

Washington, DC 20229

http://www.ice.gov

Tel: 202-344-2410

Fax: 202-344-1920

E-mail: iprcenter@dhs.gov

Joint center to coordinate interagency efforts on criminal intellectual property enforcement by ICE and the FBI.

Federal Bureau of Investigation

Cyber Crime Fraud Unit

Leslie Bryant - Chief

J. Edgar Hoover FBI Building

935 Pennsylvania Avenue NW

Washington, DC 20535

http://www.fbi.gov

Tel: 202-324-5613

Fax: 202-324-9197

E-mail: leslie.bryant@ic.fbi.gov

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 Patrol (CBP)

1300 Pennsylvania Avenue NW

Washington, DC 20229

http://www.cbp.gov/

- Office of Regulations and Rulings—IPR Branch

  Tel: 202-572-8710

  Fax: 202-572-8744

  E-mail: hqiprbranch@dhs.gov

  Develops and administers legal and policy components of the agency's IPR enforcement program.

- IPR E-Recordation (IPRR) Application

  E-mail: iprr.questions@dhs.gov

  http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ipr/iprr_intro.xml

  Online application for intellectual property owners to record their trademarks and copyrights with CBP to protect against the importation of infringing products.

- Office of Trade Relations

  Tel: 202-344-1440

  Fax: 202-344-1969

  E-mail: traderelations@dhs.gov

  http://www.cbp.gov/xp/cgov/toolbox/about/organization/comm_staff_off/trade_relations.xml

  Liaison between industry and Customs officials. Reviews concerns voiced by individuals or trade groups and furnishes recommendations to resolve justified complaints.

- Cyber Crime Center

  Cyber Crimes Unit

  1320 Random Hills Road, Suite 400

  Fairfax, VA 22030

  Tel: 703-293-8005

  Fax: 703-293-9127

  Investigates and coordinates investigation of Internet crimes, including intellectual property rights violations.

U.S. Postal Inspection Service

Mail Fraud Group

475 L'Enfant Plaza SW, Room 3411

Washington, DC 20260

Tel: 202-268-4267

Fax: 202-268-7316

http://www.usps.com/postalinspectors/

Support and oversight of Postal Inspection Service's mail fraud enforcement nationwide, including investigation of intellectual property 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: 301-294-4030

Fax: 301-594-1971

http://www.fda.gov/ora/

Support and oversight of FDA's enforcement of violations of laws related to mislabeled foods, drugs, and cosmetics.

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

E-mail: info@cpsc.gov

Dennis Blasius

Special Assistant to the Deputy Director

Office of Compliance and Field Operations

U.S. Consumer Product Safety Commission

2331 Silvernail Road #24

Pewaukee, WI 53072

Tel: 262-650-1216

Fax: 262-650-1217

Cell: 414-899-8802

E-mail: dblasius@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.

National White Collar Crime Center (NW3C)

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 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 Attache program

  Tel.: 202-514-0000

- **Office of Overseas Prosecutorial Development & Training**

  Resident Legal Advisor program

  Tel.: 202-514-1323

- **Federal Bureau of Investigation Legal Attache Program**

  http://www.fbi.gov/contact/legat/legat.htm

State Department Information on Mutual Legal Assistance Treaties

http://travel.state.gov/law/info/judicial/judicial_690.html

U.S. Trade Representative's List of Nations that Fail to Provide Adequate IP Protection

Annual Special 301 Report

http://ustr.gov/Trade_Sectors/Intellectual_Property/Section_Index.html

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

http://www.uspto.gov/

Provides information on obtaining certified copies of trademark registration. To obtain a copy of a certified trademark registration:

- Office of Public Records

  South Tower Building, 2nd Floor

  2900 Crystal Drive

  Arlington, VA 22202

  Tel.: 800-972-6382

Fax: 571-273-3250

http://www.uspto.gov

International Anti-Counterfeiting Coalition (IACC)

Niles Montan

President

1725 K Street NW, Suite 411

Washington, DC 20006

Tel.: 202-223-6667

Fax: 202-223-6668

http://www.iacc.org

Represents trademark industries affected by counterfeiting.

International Trademark Association (INTA)

Saisal Daudpota

External Relations Coordinator, Anti-Counterfeiting

655 Third Avenue, 10th Floor

New York, NY 10017-5617

Tel.: 212-642-1739

Fax: 212-768-7796

http://www.inta.org

Represents trademark owners in all industries.

4. Copyright Organization Contacts

Library of Congress Copyright Office

Certifications & Documents

LM 402

101 Independence Avenue SW

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.

The Independent Film & Television Alliance (I.F.T.A.)

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.

Association of American Publishers (AAP)

Patricia L. Judd

Executive Director

International Copyright Enforcement and Trade Policy

50 F Street NW, 4th Floor

Washington, DC 20001

Tel.: 202-220-4541

Fax: 202-347-3690

http://www.publishers.org

Represents publishers of reference works; scientific medical, technical, professional, and scholarly books and journals; and classroom instructional and testing materials in print and electronic formats.

Business Software Alliance (BSA)

John Wolfe

Director Internet Enforcement

1150 18th Street NW, Suite 700

Washington, DC 20036

Tel.: 202-872-5500; 202-872-5122

Fax: 202-872-5501

E-mail: johnw@bsa.org

http://www.bsa.org

Represents major software and e-commerce developers. 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.

Entertainment Software Association (ESA)

Chun T. Wright

Senior Anti-Piracy Counsel

575 7th Street NW, Suite 300

Washington, DC 20004

Tel.: 202-223-2400 ext. 108

Fax: 202-223-2401

E-mail: chun@theESA.com

New York office

Tel.: 917-522-3250

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.

International Intellectual Property Alliance (IIPA)

Steve Metalitz

Senior Vice President

1747 Pennsylvania Avenue NW, Suite 825

Washington, DC 20006-4637

Tel.: 202-833-4198

Fax: 202-872-0546

http://www.iipa.com

Coalition of seven U.S. associations working to improve international copyright protection and enforcement.

International Intellectual Property Institute (IIPI)

Eric Garduno

Executive Director

1100 H Street NW, Suite 1100

Washington, DC 20005

Tel.: 202-544-6610

Fax: 202-478-1955

http://www.iipi.org

Organization dedicated to improving intellectual property systems around the world.

Intellectual Property Owners Association (IPO)

Mr. Dana Robert Colarulli

Government Relations and Legislative Counsel

1255 23rd Street NW, Suite 200

Washington, DC 20037

E-mail: dana@ipo.org

Tel.: 202-466-2396

Fax: 202-466-2893

http://www.ipo.org

E-mail: info@ipo.org

Represents owners of intellectual property.

Motion Picture Association of America (MPAA)

Mike Robinson

Director of U.S. Anti-Piracy

Appendix H

Victim Referral and Witness Interview Forms

The forms on the following pages were first published in the Department of Justice's *Report of the Department of Justice's Task Force on Intellectual Property* (Oct. 2004), and are adapted below with minor additions. The forms are useful as a checklist for prosecutors and investigators to gather information from victims or for victims to fill out on their own. There are two forms: one that can be used in copyright and trademark/service mark/certification mark cases, and another that can be used in trade secret cases. They can be adapted for use in other intellectual property offenses as well, and are available in electronic format on DOJNET at http://10.173.2.12/usao/eousa/ole/usabook/ipma/appxh.wpd.

A. Checklist for Copyright Infringement and Counterfeit Trademark/Service Mark/Certification Mark Offenses

Background and Contact Information

1. Victim's Name:
2. Primary Address:
3. Nature of Business:
4. Contact:
   Phone: Fax:
   E-mail: Pager/Mobile:

Description of the Intellectual Property

5. 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 specially problematic (e.g., pre-release piracy, threats to public health and safety).

6. 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?

   ___ YES ___NO

   a. If so, please provide the following:

      i. Registration Date:

      ii. Registration Number:

      iii. Do you have a copy of the certificate of registration?

      iv. Has the work or mark been the subject of a previous civil or criminal enforcement action? If so, please provide a general description.

   b. If not, state if and when you intend to register.

7. What is the approximate retail value of the infringed work, good, or service?

Description of the Intellectual Property Crime

8. Describe how the theft or counterfeiting was discovered.

9. Do you have any examination reports of the infringing or counterfeit goods?

   ___YES ___NO

   If so, please provide those reports to law enforcement.

10. Describe the scope of the infringing operation:

    a. Estimated quantity of illegal distribution:

    b. Estimated value of illegal distribution:

    b. Estimated time period of illegal distribution:

    c. Is the illegal distribution national or international? Which states or countries?

11. Identify where the infringement or counterfeiting occurred, and describe the location.

12. Identify the name(s) or location(s) of possible suspects, including the following information:

    Name (Suspect #1):
    Phone number:
    E-mail address:
    Physical address:
    Current employer, if known:
    Reason for suspicion:

    Name (Suspect #2):
    Phone number:
    E-mail address:
    Physical address:
    Current employer, if known:
    Reason for suspicion:

13. If the distribution of infringing or counterfeit goods involves the Internet (e.g., World Wide Web, FTP, e-mail, chat rooms), identify the following:

    a. The type of Internet theft:

    b. Internet address, including linking sites (domain name, URL, IP address, e-mail):

    c. Login or password for site:

    d. Operators of site, if known:

14. 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:

Civil Enforcement Proceedings

15. Has a civil enforcement action been filed against the suspects identified above?

    ___YES ___NO

    a. If so, identify the following:

        i. Name of court and case number:

        ii. Date of filing:

        iii. Names of attorneys:

        iv. Status of case:

    b. If not, is a civil action contemplated? What type and when?

16. Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

B. Checklist for 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.

Background and Contact Information

1. Victim's Name:

2. Primary Location and Address:

3. Nature of Primary Business:

4. Law Enforcement Contact:

   Phone: Fax:

   E-mail: Pager/Mobile:

Description of the Trade Secret

5. Generally describe the trade secret (e.g., source code, formula, technology, device).

   Provide an estimated value of the trade secret identifying ONE of the methods and indicating ONE of the ranges listed below:

Estimated value	Method
_____	Cost to develop the trade secret
_____	Acquisition cost (identify date and source of acquisition)
_____	Fair market value if sold

   Identify a person knowledgeable about valuation, including that person's contact information.

General Physical Measures Taken to Protect the Trade Secret

6. Describe the general physical security precautions taken by the company, such as fencing the perimeter of the premises, visitor control systems, using alarming or self-locking doors or security personnel.

7. Has the company established physical barriers to prevent unauthorized viewing or access to the trade secret, such as locked storage facilities or "Authorized Personnel Only" signs at access points? (See below if computer-stored trade secret.)

   ___YES ___NO

8. Does the company require sign in/out procedures for access to and return of trade secret materials?

   ___YES ___NO

9. Are employees required to wear identification badges?

   ___YES ___ NO

10. Does the company have a written security policy?

    ___YES ___NO

    a. How are employees advised of the security policy?

    b. Are employees required to sign a written acknowledgment of the security policy?

       ___YES ___NO

    c. Identify the person most knowledgeable about matters relating to the security policy, including title and contact information.

11. How many employees have access to the trade secret?

12. Was access to the trade secret limited to a "need to know" basis?

    ___YES ___NO

    If so, 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.):

Confidentiality and Non-Disclosure Agreements

13. Does the company enter into confidentiality and non-disclosure agreements with employees and third parties concerning the trade secret?

    ___YES ___NO

14. Has the company established and distributed written confidentiality policies to all employees?

    ___YES ___NO

15. Does the company have a policy for advising company employees regarding the company's trade secrets?

    ___YES ___NO

Computer-Stored Trade Secrets

16. If the trade secret is computer source code or other computer-stored information, how is access regulated (e.g., are employees given unique user names, passwords, and computer storage space, and was the information encrypted)?

17. If the company stores the trade secret on a computer network, is the network protected by a firewall?

    ___YES ___NO

18. Is remote access permitted into the computer network?

    ___YES ___NO

19. Is the trade secret maintained on a separate computer server?

    ___YES ____NO

20. Does the company prohibit employees from bringing outside computer programs or storage media to the premises?

    ___YES ___NO

21. Does the company maintain electronic access records such as computer logs?

    ___YES ___NO

Document Control

22. If the trade secret consists of documents, were they clearly marked "CONFIDENTIAL" or "PROPRIETARY"?

    ___YES ___NO

23. Describe the document control procedures employed by the company, such as limiting access and sign in/out policies.

24. Was there a written policy concerning document control procedures?

    ___YES ___NO

    If so, how were employees advised of it?

25. Identify the person most knowledgeable about the document control procedures, including title and contact information.

Employee Controls

26. Are new employees subject to a background investigation?

    ___YES ___NO

27. Does the company hold "exit interviews" to remind departing employees of their obligation not to disclose trade secrets?

    ___YES ___NO

Description of the Theft of Trade Secret

28. Identify the name(s) or location(s) of possible suspects, including the following information:

    Name (Suspect #1):
    Phone number:
    E-mail address:
    Physical address:
    Employer:
    Reason for suspicion:

    Name (Suspect #2):
    Phone number:
    E-mail address:
    Physical address:
    Employer:

    Reason for suspicion:

29. Was the trade secret stolen to benefit a third party, such as a competitor or another business?

    ___YES ___NO

    If so, identify that business and its location.

30. Do you have any information that the theft of trade secrets were committed to benefit a foreign government or instrumentality of a foreign government?

    ___YES ___NO

    If so, identify the foreign government or instrumentality and describe that information.

31. If the suspect is a current or former employee, describe all confidentiality and non-disclosure agreements in effect.

32. Identify any physical locations associated with the theft of trade secret, such as where it may be currently stored or used.

33. If you have conducted an internal investigation into the theft or counterfeiting activities, please describe any evidence acquired and provide any investigative reports that you can.

Civil Enforcement Proceedings

34. Has a civil enforcement action been filed against the suspects identified above?

    ___YES ___NO

    a. If so, identify the following:

        i. Name of court and case number:

        ii. Date of filing:

        iii. Names of attorneys:

        iv. Status of case:

    b. If not, is a civil action contemplated?

        ___YES ___NO

        What type and when?

35. Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

Appendix I

Maximum Statutory Penalties, Forfeiture, and Restitution for Intellectual Property Crimes

Fines are determined by the substantive criminal statutes in conjunction with 18 U.S.C. § 3571 ("Sentence of fine").The exact forfeiture procedures for each criminal offense, and the types of property those remedies reach, are listed in detail in Section VIII.E.2. of this Manual. Restitution procedures are described in detail in Section VIII.D. of this Manual.

	Commercial Purpose[1] - 1st Offense	Commercial Purpose - 2nd Offense	No Commercial Purpose - 1st Offense	No Commercial Purpose - 2nd Offense
Copyright Infringement for Profit (Felony)[2] **17 U.S.C. § 506(a)(1)(A)** **(formerly § 506(a)(1))** **18 U.S.C. § 2319(b)**	• 5 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory	• 10 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory		

	Commercial Purpose[1] - 1st Offense	Commercial Purpose - 2nd Offense	No Commercial Purpose - 1st Offense	No Commercial Purpose - 2nd Offense
Copyright Large-Scale Infringement, No Profit Motive (Felony) **17 U.S.C. § 506(a)(1)(B)** **(formerly § 506(a)(2))** **18 U.S.C. § 2319(c)**			• 3 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory	• 6 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory
Copyright Pre-Release Distribution Over a Publicly-Accessible Computer Network **17 U.S.C. § 506(a)(1)(C)** **18 U.S.C. § 2319(d)**	• 5 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory	• 10 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory	• 3 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory	• 6 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory

	Commercial Purpose[1] - 1st Offense	Commercial Purpose - 2nd Offense	No Commercial Purpose - 1st Offense	No Commercial Purpose - 2nd Offense
Digital Millennium Copyright Act (DMCA) **17 U.S.C. § 1204**	• 5 years • $500K or twice the gain/loss (individuals & organizations) • Forfeiture–none • Restitution–none to circumvention victims; possible to copyright victims	• 10 years • $1M or twice the gain/loss (individuals & organizations) • Forfeiture–none • Restitution–none to circumvention victims; possible to copyright victims		
Economic Espionage Act (EEA)– **Trade Secret Theft to Benefit a Foreign Government, Instrumentality, or Agent[3]** **18 U.S.C. § 1831**			• 15 years • $500K or twice the gain/loss (individuals) • $10M or twice the gain/loss (organizations) • Forfeiture–crim. only • Restitution–mandatory	
Economic Espionage Act (EECA)– **Trade Secret Theft for Commercial Purposes** **18 U.S.C. § 1832**	• 10 years • $250K or twice the gain/loss (individuals) • $5M or twice the gain/loss (organizations) • Forfeiture–crim. only • Restitution–mandatory			

	Commercial Purpose[1] - 1st Offense	Commercial Purpose - 2nd Offense	No Commercial Purpose - 1st Offense	No Commercial Purpose - 2nd Offense
Counterfeit/ Illicit Labels and Counterfeit Documentation and Packaging for Copyrighted Works **18 U.S.C. § 2318**	• 5 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture– civ. & crim. • Restitution– mandatory			
Bootleg Recordings of Live Musical Performances **18 U.S.C. § 2319A**	• 5 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture– civ. & crim. • Restitution– unclear	• 10 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture– civ. & crim. • Restitution– unclear		
Camcording **18 U.S.C. § 2319B**			• 3 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture– crim. only • Restitution– mandatory	• 6 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture– crim. only • Restitution– mandatory

	Commercial Purpose[1] - 1st Offense	Commercial Purpose - 2nd Offense	No Commercial Purpose - 1st Offense	No Commercial Purpose - 2nd Offense
Counterfeit Trademarks, Service Marks, and Certification Marks **18 U.S.C. § 2320**	• 10 years • $2M or twice the gain/loss (individuals) • $5M or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory	• 20 years • $5M or twice the gain/loss (individuals) • $15M or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory		

1. "Commercial purpose" here is used as a generic term applicable to criminal intellectual property statutes that variously require the government to prove either trafficking for "consideration"; commercial advantage or private financial gain; or engaging in a transaction for economic benefit. The terms of the specific statutes control.

2. The copyright crimes in 17 U.S.C. § 506(a)(1)(A) and (B) can also be charged as misdemeanors in certain circumstances.

3. Technically, to prove economic espionage to benefit a foreign government, instrumentality, or agent under 18 U.S.C. § 1831, the government need not prove that the benefit was economic, but in practice the benefit will often have economic consequences.

15503 Ventura Boulevard

Encino, CA 91436

Tel.: 818-995-6600

Fax: 818-382-1795

Bill Shannon

Deputy Director U.S. Anti-Piracy

Tel.: 718-518-8800 ext. 108

Cell: 917-731-5783

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)

Jonathan Whitehead

Senior Vice President, Online Copyright Protection

Anti-Piracy Unit

1330 Connecticut Avenue NW, Suite 300

Washington, DC 20036

Tel.: 202-857-9602

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.

International Federation of the Phonographic Industry (IFPI)

Jeremy Banks

Vice President of Internet Anti-Piracy

IFPI Secretariat

54 Regent Street

London

W1B 5RE

United Kingdom

Tel.: 011-44-207-878-6804

E-mail: jeremy.banks@ifpi.org

http://www.ifpi.org/

Represents the worldwide recording industry's international organizations, legal strategies, litigation, and public relations. Co-ordinates international strategies in anti-piracy enforcement, technology, and lobbying of governments. IFPI and RIAA work closely together. RIAA recommends contacting it before contacting the IFPI.

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

Vice President, Intellectual Property Policy & Enforcement

Tel.: 202-789-4442

E-mail: keithk@siia.net

Jason Allen

Manager, Internet Anti-Piracy

Tel.: 202-789-4477

E-mail: jallen@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 registration certificates.

Appendix H

Victim Referral and Witness Interview Forms

The forms on the following pages were first published in the Department of Justice's *Report of the Department of Justice's Task Force on Intellectual Property* (Oct. 2004), and are adapted below with minor additions. The forms are useful as a checklist for prosecutors and investigators to gather information from victims or for victims to fill out on their own. There are two forms: one that can be used in copyright and trademark/service mark/certification mark cases, and another that can be used in trade secret cases. They can be adapted for use in other intellectual property offenses as well, and are available in electronic format on DOJNET at http://10.173.2.12/usao/eousa/ole/usabook/ipma/appxh.wpd.

A. Checklist for Copyright Infringement and Counterfeit Trademark/Service Mark/Certification Mark Offenses

Background and Contact Information

1. Victim's Name:
2. Primary Address:
3. Nature of Business:
4. Contact:
   Phone: Fax:
   E-mail: Pager/Mobile:

Description of the Intellectual Property

5. 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 specially problematic (e.g., pre-release piracy, threats to public health and safety).

6. 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?

   ___ YES ___NO

   a. If so, please provide the following:

      i. Registration Date:

      ii. Registration Number:

      iii. Do you have a copy of the certificate of registration?

      iv. Has the work or mark been the subject of a previous civil or criminal enforcement action? If so, please provide a general description.

   b. If not, state if and when you intend to register.

7. What is the approximate retail value of the infringed work, good, or service?

Description of the Intellectual Property Crime

8. Describe how the theft or counterfeiting was discovered.

9. Do you have any examination reports of the infringing or counterfeit goods?

   ___YES ___NO

   If so, please provide those reports to law enforcement.

10. Describe the scope of the infringing operation:

    a. Estimated quantity of illegal distribution:

    b. Estimated value of illegal distribution:

    b. Estimated time period of illegal distribution:

    c. Is the illegal distribution national or international? Which states or countries?

11. Identify where the infringement or counterfeiting occurred, and describe the location.

12. Identify the name(s) or location(s) of possible suspects, including the following information:

    Name (Suspect #1):
    Phone number:
    E-mail address:
    Physical address:
    Current employer, if known:
    Reason for suspicion:

    Name (Suspect #2):
    Phone number:
    E-mail address:
    Physical address:
    Current employer, if known:
    Reason for suspicion:

13. If the distribution of infringing or counterfeit goods involves the Internet (e.g., World Wide Web, FTP, e-mail, chat rooms), identify the following:

    a. The type of Internet theft:

    b. Internet address, including linking sites (domain name, URL, IP address, e-mail):

    c. Login or password for site:

    d. Operators of site, if known:

14. 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:

Civil Enforcement Proceedings

15. Has a civil enforcement action been filed against the suspects identified above?

    ___YES ___NO

    a. If so, identify the following:

        i. Name of court and case number:

        ii. Date of filing:

        iii. Names of attorneys:

        iv. Status of case:

    b. If not, is a civil action contemplated? What type and when?

16. Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

B. Checklist for 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.

Background and Contact Information

1. Victim's Name:

2. Primary Location and Address:

3. Nature of Primary Business:

4. Law Enforcement Contact:

   Phone: Fax:

   E-mail: Pager/Mobile:

Description of the Trade Secret

5. Generally describe the trade secret (e.g., source code, formula, technology, device).

   Provide an estimated value of the trade secret identifying ONE of the methods and indicating ONE of the ranges listed below:

Estimated value	Method
_____	Cost to develop the trade secret
_____	Acquisition cost (identify date and source of acquisition)
_____	Fair market value if sold

   Identify a person knowledgeable about valuation, including that person's contact information.

General Physical Measures Taken to Protect the Trade Secret

6. Describe the general physical security precautions taken by the company, such as fencing the perimeter of the premises, visitor control systems, using alarming or self-locking doors or security personnel.

7. Has the company established physical barriers to prevent unauthorized viewing or access to the trade secret, such as locked storage facilities or "Authorized Personnel Only" signs at access points? (See below if computer-stored trade secret.)

   ___YES ___NO

8. Does the company require sign in/out procedures for access to and return of trade secret materials?

   ___YES ___NO

9. Are employees required to wear identification badges?

   ___YES ___ NO

10. Does the company have a written security policy?

    ___YES ___NO

    a. How are employees advised of the security policy?

    b. Are employees required to sign a written acknowledgment of the security policy?

       ___YES ___NO

    c. Identify the person most knowledgeable about matters relating to the security policy, including title and contact information.

11. How many employees have access to the trade secret?

12. Was access to the trade secret limited to a "need to know" basis?

    ___YES ___NO

    If so, 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.):

Confidentiality and Non-Disclosure Agreements

13. Does the company enter into confidentiality and non-disclosure agreements with employees and third parties concerning the trade secret?

    ___YES ___NO

14. Has the company established and distributed written confidentiality policies to all employees?

    ___YES ___NO

15. Does the company have a policy for advising company employees regarding the company's trade secrets?

    ___YES ___NO

Computer-Stored Trade Secrets

16. If the trade secret is computer source code or other computer-stored information, how is access regulated (e.g., are employees given unique user names, passwords, and computer storage space, and was the information encrypted)?

17. If the company stores the trade secret on a computer network, is the network protected by a firewall?

    ___YES ___NO

18. Is remote access permitted into the computer network?

    ___YES ___NO

19. Is the trade secret maintained on a separate computer server?

    ___YES ____NO

20. Does the company prohibit employees from bringing outside computer programs or storage media to the premises?

    ___YES ___NO

21. Does the company maintain electronic access records such as computer logs?

    ___YES ___NO

Document Control

22. If the trade secret consists of documents, were they clearly marked "CONFIDENTIAL" or "PROPRIETARY"?

    ___YES ___NO

23. Describe the document control procedures employed by the company, such as limiting access and sign in/out policies.

24. Was there a written policy concerning document control procedures?

    ___YES ___NO

    If so, how were employees advised of it?

25. Identify the person most knowledgeable about the document control procedures, including title and contact information.

Employee Controls

26. Are new employees subject to a background investigation?

    ___YES ___NO

27. Does the company hold "exit interviews" to remind departing employees of their obligation not to disclose trade secrets?

    ___YES ___NO

Description of the Theft of Trade Secret

28. Identify the name(s) or location(s) of possible suspects, including the following information:

    Name (Suspect #1):
    Phone number:
    E-mail address:
    Physical address:
    Employer:
    Reason for suspicion:

    Name (Suspect #2):
    Phone number:
    E-mail address:
    Physical address:
    Employer:

    Reason for suspicion:

29. Was the trade secret stolen to benefit a third party, such as a competitor or another business?

    ___YES ___NO

    If so, identify that business and its location.

30. Do you have any information that the theft of trade secrets were committed to benefit a foreign government or instrumentality of a foreign government?

    ___YES ___NO

    If so, identify the foreign government or instrumentality and describe that information.

31. If the suspect is a current or former employee, describe all confidentiality and non-disclosure agreements in effect.

32. Identify any physical locations associated with the theft of trade secret, such as where it may be currently stored or used.

33. If you have conducted an internal investigation into the theft or counterfeiting activities, please describe any evidence acquired and provide any investigative reports that you can.

Civil Enforcement Proceedings

34. Has a civil enforcement action been filed against the suspects identified above?

    ___YES ___NO

    a. If so, identify the following:

        i. Name of court and case number:

        ii. Date of filing:

        iii. Names of attorneys:

        iv. Status of case:

    b. If not, is a civil action contemplated?

        ___YES ___NO

        What type and when?

35. Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

Appendix I

Maximum Statutory Penalties, Forfeiture, and Restitution for Intellectual Property Crimes

Fines are determined by the substantive criminal statutes in conjunction with 18 U.S.C. § 3571 ("Sentence of fine").The exact forfeiture procedures for each criminal offense, and the types of property those remedies reach, are listed in detail in Section VIII.E.2. of this Manual. Restitution procedures are described in detail in Section VIII.D. of this Manual.

	Commercial Purpose[1] - 1st Offense	Commercial Purpose - 2nd Offense	No Commercial Purpose - 1st Offense	No Commercial Purpose - 2nd Offense
Copyright Infringement for Profit (Felony)[2] **17 U.S.C. § 506(a)(1)(A)** **(formerly § 506(a)(1))** **18 U.S.C. § 2319(b)**	• 5 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory	• 10 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory		

	Commercial Purpose[1] - 1st Offense	Commercial Purpose - 2nd Offense	No Commercial Purpose - 1st Offense	No Commercial Purpose - 2nd Offense
Copyright Large-Scale Infringement, No Profit Motive (Felony) **17 U.S.C. § 506(a)(1)(B)** **(formerly § 506(a)(2))** **18 U.S.C. § 2319(c)**			• 3 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory	• 6 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory
Copyright Pre-Release Distribution Over a Publicly-Accessible Computer Network **17 U.S.C. § 506(a)(1)(C)** **18 U.S.C. § 2319(d)**	• 5 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory	• 10 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory	• 3 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory	• 6 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory

	Commercial Purpose[1] - 1st Offense	Commercial Purpose - 2nd Offense	No Commercial Purpose - 1st Offense	No Commercial Purpose - 2nd Offense
Digital Millennium Copyright Act (DMCA) **17 U.S.C. § 1204**	• 5 years • $500K or twice the gain/loss (individuals & organizations) • Forfeiture–none • Restitution–none to circumvention victims; possible to copyright victims	• 10 years • $1M or twice the gain/loss (individuals & organizations) • Forfeiture–none • Restitution–none to circumvention victims; possible to copyright victims		
Economic Espionage Act (EEA)– **Trade Secret Theft to Benefit a Foreign Government, Instrumentality, or Agent[3]** **18 U.S.C. § 1831**			• 15 years • $500K or twice the gain/loss (individuals) • $10M or twice the gain/loss (organizations) • Forfeiture–crim. only • Restitution–mandatory	
Economic Espionage Act (EECA)– **Trade Secret Theft for Commercial Purposes** **18 U.S.C. § 1832**	• 10 years • $250K or twice the gain/loss (individuals) • $5M or twice the gain/loss (organizations) • Forfeiture–crim. only • Restitution–mandatory			

	Commercial Purpose[1] - 1st Offense	Commercial Purpose - 2nd Offense	No Commercial Purpose - 1st Offense	No Commercial Purpose - 2nd Offense
Counterfeit/ Illicit Labels and Counterfeit Documentation and Packaging for Copyrighted Works **18 U.S.C. § 2318**	• 5 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture– civ. & crim. • Restitution– mandatory			
Bootleg Recordings of Live Musical Performances **18 U.S.C. § 2319A**	• 5 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture– civ. & crim. • Restitution– unclear	• 10 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture– civ. & crim. • Restitution– unclear		
Camcording **18 U.S.C. § 2319B**			• 3 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture– crim. only • Restitution– mandatory	• 6 years • $250K or twice the gain/loss (individuals) • $500K or twice the gain/loss (organizations) • Forfeiture– crim. only • Restitution– mandatory

	Commercial Purpose[1] - 1st Offense	Commercial Purpose - 2nd Offense	No Commercial Purpose - 1st Offense	No Commercial Purpose - 2nd Offense
Counterfeit Trademarks, Service Marks, and Certification Marks **18 U.S.C. § 2320**	• 10 years • $2M or twice the gain/loss (individuals) • $5M or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory	• 20 years • $5M or twice the gain/loss (individuals) • $15M or twice the gain/loss (organizations) • Forfeiture–civ. & crim. • Restitution–mandatory		

1. "Commercial purpose" here is used as a generic term applicable to criminal intellectual property statutes that variously require the government to prove either trafficking for "consideration"; commercial advantage or private financial gain; or engaging in a transaction for economic benefit. The terms of the specific statutes control.

2. The copyright crimes in 17 U.S.C. § 506(a)(1)(A) and (B) can also be charged as misdemeanors in certain circumstances.

3. Technically, to prove economic espionage to benefit a foreign government, instrumentality, or agent under 18 U.S.C. § 1831, the government need not prove that the benefit was economic, but in practice the benefit will often have economic consequences.

Appendix J

Examples of Traditional Assistance and Gifts to Law Enforcement

The examples below of what constitutes a gift or traditional assistance to law enforcement 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 address 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 Scenario #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 they 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

COPYRIGHT

WRIT OF MANDAMUS
see MANDAMUS