PROSECUTING INTELLECTUAL PROPERTY CRIMES

November 2000

Computer Crime & Intellectual Property Section, Criminal Division
U.S. Department of Justice

PREFACE

This manual represents a comprehensive, up-to-date resource for prosecution of intellectual property crimes. The present edition is a thorough revision of the previous one, issued in 1997. The edition addresses many legislative developments that have taken place since the previous manual was published. It also provides substantial practical guidance for prosecutors and in-depth coverage of experiences gained from the prosecution of high-technology cases.

Since the 1997 edition, the major developments relating to codified law are as follows:

- A detailed analysis of the revised criminal copyright statutes, 17 U.S.C. § 506 and 18 U.S.C. § 2319, as amended by the No Electronic Theft Act of 1997
- A review of recently enacted protections used for systems of disseminating intellectual property, such as cable and satellite systems, and the recently enacted anti-circumvention crimes, 17 U.S.C. §§ 1201-1202
- An analysis of the recently updated Guideline section, U.S. Sentencing Commission, Guidelines Manual § 2B5.3(b)(1) (Nov. 1998 & Supp. 2000)

This manual also newly addresses certain prosecutorial practice areas as they relate to intellectual property cases, including:

- A discussion and framework for analyzing whether to prosecute an infringement crime, including a detailed examination of whether to charge corporations
- An expanded discussion of other federal offenses to consider in intellectual property cases, including mail and wire fraud, RICO, and money laundering
- A discussion of the victim's role in intellectual property cases
- An analysis of restitution in intellectual property cases

Finally, this edition reflects significantly more experience in prosecuting high-technology intellectual property cases. This experience is especially reflected by new or expanded sections on the following specialized subjects:

- A discussion of the legal and practical issues surrounding defendants who traffic in counterfeit goods that are comparable to legitimate goods, including a case study of computer chip remarking

- An overview of legal, technical and policy implications of copyright infringement facilitated by the Internet
- A significantly expanded discussion of 18 U.S.C. § 2318, trafficking in counterfeit labels, which has proven to be a valuable charge in copyright cases
- A discussion of the major lessons of the federal trade secret prosecutions that have arisen over the past four years since enactment of the Economic Espionage Act, 18 U.S.C. §§ 1831-1839

We hope that this edition of the manual will be a useful resource. We will make it, and any future amendments or supplements available on our Web site, http://www.cybercrime.gov. In order for us to stay abreast of the current developments in this rapidly evolving area of the law, we would like to hear about prosecutions involving the criminal intellectual property statutes. Prosecutors interested in advice beyond this manual or support on intellectual property cases are welcome to contact us as well. We would also be interested in any comments, corrections, or contributions regarding this manual. We may be reached by phone at (202) 514-1026.

The primary author and editor of this manual is David Goldstone. He worked under the supervision of Martha Stansell-Gamm, Chief; David Green, Principal Deputy Chief; and Christopher Painter, Deputy Chief, of the Computer Crime and Intellectual Property Section. Development of this manual has been a major undertaking of the Section as a whole, and substantial contributions were made by the following Section attorneys and paralegals (in alphabetical order): Kathleen Baker, Jessica Herrera, Cary Kadlecek, Stacey Levine, Jennifer Martin, Joe Metcalfe, Michael O'Leary, Richard Salgado, Michael Sussmann. Substantial contributions were also made by attorneys and interns formerly with the Section including (in alphabetical order): Christian Genetski, Susan Koeppen, Stevan Mitchell, Amanda Schreiber, Michael Stoer, Susan Wilson, and Marc Zwillinger. Helpful feedback was provided by Scott Christie, Stephen Heymann, and Fred Williams, Computer Telecommunications Coordinators at United States Attorneys' Offices. The manual owes a special debt to a previous edition, which was written in 1997 by Stevan Mitchell and Peter Toren, with the assistance of David Green. A precursor to that edition, a monograph on criminal copyright prosecutions, was published by the General Litigation and Legal Advice Section in 1989.

Quick Reference Sheet of Felony Charges to Consider and Relevant Issues to Consider in Typical Intellectual Property Cases				
Typical fact pattern	**Possible felony charge(s) and thumbnail summary of elements (for full scope, see the Manual)**	**Key questions relating to essential elements**	**Other possible strategic issues**	**IP Manual sections, forms and contacts**
"The Case of the Cache of Counterfeit Clutches" - Defendant manages an inventory of counterfeit brand-name purses and watches that fills a warehouse	**18 U.S.C. § 2320** 1. "Trafficked" in goods or services 2. Trafficking was "intentional" 3. Used a "counterfeit mark" on goods 4. Def. "knowingly used" the counterfeit mark	- What degree of control did particular individuals exercise over the goods in the warehouse? - How to show defendant's knowledge that the goods are marked with a counterfeit mark? Are the goods being marked or boxed in the warehouse? - Are the goods marked with spurious marks substantially similar to federally registered marks for the same goods?	- Will the evidence (e.g. business records) of the scale of the enterprise's operations be sufficient to provide the basis for an appropriate sentence? If not, consider charging money laundering or RICO	Ch. II (Trademark counterfeiting) Sec. VII.A (Sentencing guidelines); Sec. VI.B (Other federal offenses) Forms: App. B Contact: IACC
"Web Site O'Music" - Defendant operates a Web site providing unlimited access to albums of music by popular artists for only $10 per "subscriber"	**18 U.S.C. § 2319 & 17 U.S.C. § 506** 1. A valid copyright 2. Defendant infringed of the copyright (by reproduction or distribution) 3. Willfulness 4. Defendant infringed > 9 copies of copyrighted works with a total retail value > $2,500 within a 180-day period	- Who controlled the Web site? How can it be tied to an individual person? - For which of the songs are the copyrights actually registered? - Did the defendant have the mens rea to infringe "willfully"? - Reproduction and distribution are central to the process - How can the reproduction or distribution of $2,500 of songs within the 6 month period actually be shown?	- Are there records of quantities downloaded from this Web site in a six month period? If not, consider process to determine quantities, e.g., a 2703(d) order for past traffic or a pen/trap order to for future traffic - Internet atmospherics	Ch. III (Copyright infringement) Sec. III.E (Internet issues) Forms: App. C Contact: RIAA
"Buying the Beatles at the Flea market" (Count option #1) - Defendant operates a flea market booth each week where he sells pirated audio tapes of popular music	**18 U.S.C. § 2319 & 17 U.S.C. § 506** 1. A valid copyright 2. Defendant infringed of the copyright (by reproduction or distribution) 3. Willfulness 4. Defendant infringed > 9 copies of copyrighted works with a total retail value > $2,500 within a 180-day period	- Is the music copyrighted? - Did the defendant have the mens rea to infringe "willfully"? - Reproduction is copying and creating the tapes, whereas distribution is selling them - How can the reproduction or distribution of $2,500 of songs within the 6 month period actually be shown?	- If defendant is just selling them, he may be part of a conspiracy including a large-scale copying operation - Or he might be able to provide information regarding the source of the pirated music	Ch. III (Copyright infringement) Forms: App. C Contact: RIAA

Quick Reference Sheet of Felony Charges to Consider and Relevant Issues to Consider in Typical Intellectual Property Cases				
Typical fact pattern	**Possible felony charge(s) and thumbnail summary of elements (for full scope, see the Manual)**	**Key questions relating to essential elements**	**Other possible strategic issues**	**IP Manual sections, forms and contacts**
"Buying the Beatles at the Flea market" (Count option #2) - Defendant operates a flea market booth each week where he sells pirated audio tapes of popular music	**18 U.S.C. § 2318** 1. Trafficking in labels affixed or designed to be affixed to a phonorecord or other audiovisual work 2. The labels/documentation were counterfeit 3. The defendant acted "knowingly" 4. The work is copyrighted	- Is the music labeled with a counterfeit label, i.e., a label that is not genuine? - Did the defendant know the label was counterfeit? - Is the music copyrighted? - Does the defendant aware that he is trafficking in such goods?	- Note that the defendant is "trafficking" in the goods in the defendant's possession even if not yet sold so long as the defendant has control with intent to transfer them to others - If marked with a trademark, consider 18 U.S.C. § 2320	Ch. IV (Counterfeit labeling) Forms: App. D Contact: RIAA
"Case of the candid car-part counterfeiter" Defendant is selling used automobile parts in counterfeit boxes (which he orders from the printer to look legitimate) after testing them to automotive mechanics shops and telling that the parts are "not quite brand new, but just as good" Defendant also sells excess counterfeit boxes without parts in them.	**18 U.S.C. § 2320** 1. "Trafficked" in goods 2. Trafficking was "intentional" 3. Used a "counterfeit mark" on goods 4. Def. "knowingly used" the counterfeit mark	- Defendant is clearly intentionally trafficking in the automobile parts - Are the counterfeit boxes indeed marked with a counterfeit mark substantially similar to the genuine auto part mark that could lead to downstream consumer confusion? Were they marked in a way to clarify that they had been used and repackaged and would not properly be subject to customer support or warranty coverage as that provided by the mark holder? - Did the defendant compensate (or even notify) the auto part mark holder? - Did the defendant invite any third party to investigate whether the quality control procedures, if any, used were equivalent to those used by the auto part mark holder?	- A counterfeiting case does not require a fraud on the immediate purchaser, even where the goods are comparable to legit. goods - Under USSG § 2B5.3(B)(4), the offense level may be increased by 2 (up to 13 at a minimum) if the offense involved the conscious or reckless risk of serious bodily injury. - Restitution may be significant - The sale of the excess boxes may not by itself violate 2320 but it is a great lead the b/c (1) the customer may be violating 2320 and (2) the sale may constitute aiding and abetting or participation in a conspiracy.	Ch. II (Trademark counterfeiting) Sec. II.E (Comparable goods) Sec. VII.B (Restitution) Forms: App. B Contact: IACC

Quick Reference Sheet of Felony Charges to Consider and Relevant Issues to Consider in Typical Intellectual Property Cases				
Typical fact pattern	**Possible felony charge(s) and thumbnail summary of elements (for full scope, see the Manual)**	**Key questions relating to essential elements**	**Other possible strategic issues**	**IP Manual sections, forms and contacts**
"Case of the souped-up computer chips" Defendant is buying legitimate trademarked brand-name computer chips, modifying them to permit operation at a higher speed than that for which they are marked, remarking them to reflect the faster speed, and selling them in counterfeit boxes identifying them as operating as remarked.	**18 U.S.C. § 2320** 1. "Trafficked" in goods 2. Trafficking was "intentional" 3. Used a "counterfeit mark" on goods 4. Def. "knowingly used" the counterfeit mark	- Defendant is clearly intentionally trafficking in the computer chips - Are the chips marked with the name-brand mark, either that had been placed on it under the supervision of the mark holder prior to being re-marked or re-placed on there by the remarker. - See other questions above under "case of the candid car part counterfeiter", e.g., regarding counterfeit markings on the box, notification of repackaging, customer support and warrantee issues, notification and compensation of the mark holder, and quality control comparison with that done by the mark holder.	- A counterfeiting case does not require a fraud on the immediate purchaser, even where the goods are comparable to legit. goods - Restitution may be significant - Duplication of copyrighted instruction manuals, if any, packaged with the chips may be a violation of 18 U.S.C. § 2319 and 17 U.S.C. § 506. - If there are identifiable, deceived consumer victims, consider charging wire or mail fraud, 18 U.S.C. §§ 1341, 1343	Ch. II (Trademark counterfeiting); Sec. II.E (Comparable goods); Sec. II.E.2 (Remarked computer chips) Sec. VII.B (Restitution) Forms: App. B Contact: IACC
"Case of the Shrink-wrapper deluxe" (Charging option #1) Defendant's company purchases counterfeit boxes for software as well as counterfeit manuals from a printer, copies commercial software onto CD-ROMs, and then packages the CD-ROMs and the manuals in the packaging, and then sell it at wholesale prices to retail outlets.	**18 U.S.C. § 2320** 1. "Trafficked" in goods or services 2. Trafficking was "intentional" 3. Used a "counterfeit mark" on goods 4. Def. "knowingly used" the counterfeit mark	- Was there a counterfeit trademark on the box or the manual? - Was the mark substantially similar to an authentic mark? - Is there evidence that the packages were intended to be sold? - Is there evidence that the defendant exercised control over the goods? - Is there evidence that the defendant knew the mark was counterfeit?	- Is there a corporate defendant? - If there are individual victims who are defrauded, consider mail or wire fraud, 18 U.S.C. § 1341, 1343	Ch. II (Trademark counterfeiting) Sec. VI.A.4 (Charging corporations in IP cases) Forms: App. B Contact: BSA, SIIA

Quick Reference Sheet of Felony Charges to Consider and Relevant Issues to Consider in Typical Intellectual Property Cases				
Typical fact pattern	**Possible felony charge(s) and thumbnail summary of elements (for full scope, see the Manual)**	**Key questions relating to essential elements**	**Other possible strategic issues**	**IP Manual sections, forms and contacts**
"Case of the Shrink-wrapper deluxe" (Charging option #2 - in addition to or instead of charging options # 1 & #3)	**18 U.S.C. § 2319** 1. A valid copyright 2. Defendant infringed of the copyright (by reproduction or distribution) 3. Willfulness 4. Defendant infringed > 9 copies of copyrighted works with a total retail value > $2,500 within a 180-day period	- Is the software copyrighted? - Did the defendant have the mens rea to infringe "willfully"? - Reproduction is copying and creating the CD-ROMs, whereas distribution is selling them - How can the reproduction or distribution of $2,500 of software within the 6 month period actually be shown?	- Will the evidence (e.g. business records) of the scale of the enterprise's operations be sufficient to provide the basis for an appropriate sentence? If not, consider charging money laundering or RICO - Equipment used for copyright infringement may be forfeited	Ch. III (Copyright infringement) Sec. VII (Forfeiture in IP cases) Forms: App. C Contact: BSA, SIIA
"Case of the Shrink-wrapper deluxe" (Charging option #3 - in addition to or instead of charging options #1 & #2)	**18 U.S.C. § 2318** 1. Trafficking in labels affixed or designed to be affixed to a computer program or computer software documentation 2. The labels/documentation were counterfeit 3. The defendant acted "knowingly" 4. The work is copyrighted	- Is the software copyrighted? - Are the labels (i.e., the boxes) counterfeit? - Is there evidence that the packages were intended to be sold? - Is there evidence that the defendant exercised control over the goods? - Is there evidence that the defendant knew the label was counterfeit?	- Note that the manuals could be the subject of another charge if they are copyrighted and they are counterfeit.	Ch. IV (Counterfeit labeling) Forms: App. D Contact: SIIA, BSA
"Case of economic espionage engaged by an ex-employee" Defendant uses corporate secrets of his former employer (relating to design of widgets) when working at a competitor; former employer sues defendant and competitor and reports case to federal law enforcement	**18 U.S.C. § 1832** 1. Misappropriation of information 2. Information is a trade secret 3. Def. knew it was a trade secret 4. Defendant intended that it benefit a third party 5. Defendant knew the owner of the trade secret would be injured 6. Trade secret related to a product produced for or placed in interstate or foreign commerce	- Did the defendant obtain the information by misappropriating it from the former employer? - Was the information really a trade secret? That is, did the owner take "reasonable measures" to keep it secret; and does it have "independent economic value" from being kept secret? - Are the widgets sold in interstate commerce?	- Even if crime is not completed, attempts are criminalized under 18 U.S.C. § 1832(a)(4) - Use confidentiality provisions under 18 U.S.C. § 1835 to protect the victim - Be careful not to be drawn into a commercial dispute - Remember to get DOJ approval before filing charges, at least until October 11, 2001	Ch. VIII (Trade Secret Theft) Sec. VIII.B.2.c (Trade Secret definition) Forms: App. E

TABLE OF CONTENTS

INTRODUCTION

Over the past two decades, systematic misappropriation of intellectual property has become a major concern to American businesses, artists, and authors. As the modern economy grows increasingly reliant on intellectual property, the proliferation of computers and computer networks has made the illegal reproduction and distribution of protected material much easier to accomplish. Congress has enacted workable criminal laws prohibiting such misappropriation.

This manual begins in Chapter I at page 10 with an overview of the legal protection of intellectual property. It first provides general background on intellectual property and the legal regimes employed to encourage its creation. It then explains the criminal law's role in addressing intellectual property misappropriation with a special focus on the recent Intellectual Property Rights Initiative.

The manual then discusses the criminal provisions that apply to intellectual property infringement. Among the most significant provisions are:

- Trademark counterfeiting, set out at 18 U.S.C. § 2320. See infra Chapter II at page 15;
- Infringement of copyrighted works, criminalized by 17 U.S.C. § 506(a) and 18 U.S.C. § 2319. See infra Chapter III at page 34;
- Counterfeit labeling at 18 U.S.C. § 2318. See infra Chapter IV at page 66; and
- Theft of trade secrets, prohibited by 18 U.S.C. §§ 1831 and 1832. See infra Chapter VIII at page 124.

Cutting-edge intellectual property issues, such as counterfeiting of comparable goods and Internet piracy are also discussed in detail. See infra Section II.E at page 27 (counterfeiting of comparable goods); Section III.E at page 56 (novel copyright infringement issues related to the Internet). There is also a section on other federal laws that specifically protect intellectual property or the integrity of the intellectual property rights system, such as protections for means of disseminating intellectual property, such as cable and satellite systems, and anti-circumvention devices. See infra Chapter V at page 70.

Chapter VI provides guidance on charging and other strategic issues in infringement cases, including whether to charge an infringement case, other charges to consider (such as wire and mail fraud, RICO, and money laundering), how to charge an infringement case, and the role of a victim in putting a case together. See infra Chapter VI at page 81. Chapter VII discusses the consequences of intellectual property crime. Specifically, Chapter VII provides an analysis of the United States Sentencing Guidelines ("the Guidelines"), restitution, and forfeiture issues in intellectual property cases. See infra Chapter VII at page 108.

Finally, Chapter VIII discusses the prosecution of trade secret theft and analyzes the Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-1839. Note that until October 11, 2001, all

prosecutions under this Act must first be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General of the Criminal Division. See Chapter VIII at page 124.

This manual also provides resources in the appendicies. Attached as appendices to the manual are a list of contact persons and organization (Appendix A at page 159), model indictments and jury instructions for cases under 18 U.S.C. §§ 1831-1832, 2318-2320 (Appendicies B-E at pages 165 to 184), and a listing of relevant state statutes (Appendix F at page 189).

Prosecutors may find other resources to be helpful as well, including treatises, see, e.g., J. Thomas McCarthy, McCarthy on Trademarks and Unfair Competition (1995); Roger Milgrim, Milgrim on Trade Secrets (1994); Melville B. Nimmer & David Nimmer, Nimmer on Copyright (perm. ed. rev. vol. 1999). Law review articles may also be of assistance. See, e.g., Michael Coblenz, Intellectual Property Crimes, 9 Alb. L.J. Sci. & Tech. 235 (1999); Randy Gidseg et al., Intellectual Property Crimes, 36 Am. Crm. L. Rev. 835 (1999). Legislative history for intellectual property statutes may be accessed on the Web site of the Computer Crime and Intellectual Property Section, <http://www.cybercrime.gov>, or the Web site of the Library of Congress, <http://thomas.loc.gov>.

This text is intended to be helpful to prosecuting intellectual property crime. It is not intended to create or confer any rights, privileges or benefits to prospective or actual witnesses or defendants. It is also not intended to have the force of law or of a United States Department of Justice directive. See United States v. Caceres, 440 U.S. 741 (1979).

OVERVIEW OF INTELLECTUAL PROPERTY CRIMES

This overview is provided for ease of reference to readers of this manual. It provides the essential information about most of the intellectual property crimes discussed in this manual, as well as an index into the manual to the section at which those crimes are discussed.

Trafficking in Counterfeit Goods or Services
18 U.S.C. § 2320; see Ch. II, p. 15

Elements:

1. That the defendant "trafficked" or "attempted to traffic" in goods or services;
2. That the defendant's trafficking was "intentional";
3. That the defendant used a "counterfeit mark" on or in connection with goods or services; and
4. That the defendant "knowingly used" the counterfeit mark.

Counterfeit mark:

> "a spurious mark– (i) that is used in connection with trafficking in goods or services; (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; and (iii) 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 10 copies but made 1,000)
Gray market goods:	Goods legitimately manufactured and sold overseas and then imported into U.S. outside traditional distribution channels

Statutory maximum penalties:

First offense:	10 years' imprisonment and $2,000,000 fine (individual) or $5,000,000 fine (corporation)

Guideline section: United States Sentencing Guideline § 2B5.3

Criminal Copyright Infringement
17 U.S.C. § 506(a) & 18 U.S.C. § 2319; see Ch. III, p. 34

Base felony elements (17 U.S.C. § 506(a)(2) & 18 U.S.C. § 2319(c)(1)):

1. That a copyright exists;
2. That the defendant infringed the copyright (by reproduction or distribution of the copyrighted work);

3. That the defendant acted "willfully";
4. The defendant infringed at least 10 copies of copyrighted works with a total retail value of more than $2,500 within a 180-day period.

Enhancing element (17 U.S.C. § 506(a)(2), 18 U.S.C. § 2319(c)(1)):

- Done for purposes of commercial advantage or private financial gain

Misdemeanor elements:

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) & 18 U.S.C. § 2319(c)(3)); OR
   (b) by reproduction or distribution of works with a total retail value of more than $1,000 within a 180-day period (17 U.S.C. § 506(a)(2) & 18 U.S.C. § 2319(c)(3)).

Defenses:

First Sale: The first purchaser and any subsequent purchaser of that specific copy of a copyrighted work receive the right to sell, display or dispose of their copy. If copyright owner A sells a copy of a work to B, B may sell that particular copy without violating the law. B does not, however, receive the right to reproduce and distribute additional copies made from that work.

Fair Use: Generally, the fair use doctrine excepts the otherwise infringing use of a work where it is used for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research.

Statutory maximum penalties:	First offense	Subsequent offense
Base felony	3 years, $250,000	6 years, $250,000
Felony with enhancing element	5 years, $250,000	10 years, $250,000
Misdemeanor	1 year, $100,000	1 year, $100,000

Guideline section: United States Sentencing Guideline § 2B5.3

Trafficking in Counterfeit Labels
18 U.S.C. § 2318; see Ch. IV, p. 66

Elements:

1. That the defendant acted "knowingly";
2. That the defendant trafficked in labels affixed or designed to be affixed to a phonorecord, a computer program or other audiovisual work or computer software documentation or packaging;

3. That the labels were counterfeit, i.e., an identifying label or container that appears to be genuine but is not; and
4. Federal jurisdiction is appropriate because the work (or the computer software's documentation or packaging) is federally copyrighted or for other reasons, i.e., interstate nexus (use or intent to use mail or facility of interstate commerce to commit offense), or occurring within special maritime or territorial jurisdiction of U.S.

Statutory maximum penalties: 5 years' imprisonment and $250,000 fine

Guideline section: United States Sentencing Guideline § 2B5.3

Bootleg Recordings Cases

Trafficking in Recordings of Live Musical Performances
18 U.S.C. § 2319A; see Sec. V.A.1, p. 70

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: 5 years' imprisonment and $250,000 fine (first offense)

Guideline section: United States Sentencing Guideline § 2B5.3

Television Signal De-Scrambler Cases

Federal Mail and Wire Fraud Statutes
18 U.S.C. §§ 1341, 1343; see Sec. V.B.1, p. 73

Prohibition on Devices to Intercept Communications
18 U.S.C. § 2512; see Sec. V.B.2, p. 73

Offense: Any person who intentionally--
(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the

surreptitious interception of wire, oral, or electronic communications; or (b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce

Statutory maximum penalties: 5 years' imprisonment and $250,000 fine

Guideline section: United States Sentencing Guideline § 2H3.2

Unauthorized Reception of Cable Service
47 U.S.C. § 553; see Sec. V.B.3, p.74

Offense: No person shall intercept or receive or assist in intercepting or receiving any communications service offered over a cable system, unless specifically authorized to do so by a cable operator or as may otherwise be specifically authorized by law.

Enhancement: Done willfully and for purposes of commercial advantage or private financial gain

Statutory maximum base penalties: Six months' imprisonment and $1,000 fine

Enhanced penalties: 2 years' imprisonment and $50,000 fine (first offense)

Guideline section: United States Sentencing Guideline § 2B5.3

Unauthorized Publication or Use of Communications
47 U.S.C. § 605(e)(4); see Sec. V.B.4, p. 75

Offense: Any person who manufactures, assembles, modifies, imports, exports, sells, or distributes any electronic, mechanical, or other device or equipment, knowing or having reason to know that the device or equipment is primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite services

Statutory maximum penalties: 5 years' imprisonment and $500,000 fine

Guideline section: United States Sentencing Guideline §§ 2B5.3, 2H3.1

Systems of Copyright Protection and Management

Protected by the anti-circumvention provisions of the Digital Millennium Copyright Act
17 U.S.C. §§ 1201(a)(1)-(2), (b), 1202(a)-(b); see Sec. V.C, p. 75

Criminal penalties are provided at 17 U.S.C. § 1704:

Offense: Any person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain. Generally, section 1201 outlaws circumvention of copyright protection systems; subsection 1201(a)(1) prohibits circumvention of technological measures to control access to copyrighted works; subsections 1201(a)(2) and 1201(b) prohibit trafficking in technologies that are primarily designed to circumvention of such technological measures or technological measures that protects a copyright owners' rights. Section 1202 protects the integrity of copyright management information, with subsection 1202(a) prohibiting provision or distribution of false copyright management information and 1202(b) prohibiting removal or alteration of copyright management information

Statutory maximum penalties: 5 years' imprisonment and $500,000 fine (first offense)

Commercial Theft of Trade Secrets
18 U.S.C. § 1832; see Ch. VIII, p. 124

Elements:

1. That the defendant stole, appropriated, copied, conveys, etc. without authorization information from the owner;
   Or the defendant receives, buys, possesses, etc. a trade secret knowing that it was stolen, appropriated, obtained without authorization;
   Or attempted or conspired to do the same;
2. That the defendant knew or had a firm belief that the information stolen was a trade secret;
3. For a completed offense, that the information was in fact a trade secret;
4. That the defendant intended to convert the trade secret to the economic benefit of anyone other than the owner;
5. That the defendant intended or knew the theft would injure the owner of the trade secret; and
6. That the trade secret was related to or was included in a product that was produced or placed in interstate or foreign commerce.

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

Pre-Indictment Approval Required:
Approval of Attorney General, Deputy Attorney General or Assistant Attorney General of the Criminal Division required for prosecutions brought prior to October 11, 2001; Computer Crime & Intellectual Property Section coordinates requests for approval.

Statutory maximum penalties:
10 years' imprisonment and $250,000 fine (individual); $5 million fine (corporation)

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

Foreign Economic Espionage
18 U.S.C. § 1831; see Ch. VIII, p. 124

Offense: 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, conveys, etc. 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 as (1) through (3) or (5) conspires to commit (and does an act to effect) any offense described as (1) through (3)

Pre-Indictment Approval Required:
Approval of Attorney General, Deputy Attorney General or Assistant Attorney General of the Criminal Division required for prosecutions brought prior to October 11, 2001; Internal Security Section coordinates requests for approval.

Statutory maximum penalty:
15 years' imprisonment and $500,000 fine (individual); $10 million fine (corporation)

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

Obtaining Information in Excess of Authorization by Means of a Protected Computer
18 U.S.C. § 1030(a)(2); see Sec. VIII.D.1, p. 152

Offense: Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information–

(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 (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 imprisonment and $100,000 fine

Enhanced statutory maximum penalty: 5 years' imprisonment and $250,000 fine (first offense)

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

Access of a Protected Computer with Intent to Defraud and Obtaining Something of Value
18 U.S.C. § 1030(a)(4); see Sec. VIII.D.1, p. 152

Offense: Whoever knowingly and with intent to defraud, accesses 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: Five years' imprisonment and $250,000 fine (first offense)

Guideline section: United States Sentencing Guideline § 2F1.1 (six-month minimum)

I. THE LAW'S PROTECTION OF INTELLECTUAL PROPERTY – AN OVERVIEW

Intellectual property, sometimes referred to as "IP," is an increasingly important part of the United States' economy. In 1996, the United States creative industries accounted for 3.65 percent of the gross domestic product, which is equivalent to $278.4 billion. S. Rep. No. 105-190, at 10 (1998). As the nation continues to shift from an industrial economy to an information-based economy, the assets of the country are increasingly based in intellectual property. The United States already leads the world in the creation and export of intellectual property and IP-related products. 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).

This chapter will provide an an overview of the legal protection of intellectual property. It first provides general background on intellectual property and the legal regimes employed to encourage its creation. It will explain how intellectual property may be misappropriated, and will discuss the criminal law's role in addressing intellectual property misappropriation. Finally, this chapter will provide a brief summary of the recent Intellectual Property Rights Initiative.

A. What Is "Intellectual Property" and What Are "Intellectual Property Rights"?

Legal regimes have created enforceable rights in certain intangibles that have become familiar as intellectual property, including copyrights, trademarks, patents, and trade secrets. For example, the law of copyright provides federal legal protection for infringement of certain exclusive rights, such as reproduction and distribution, of certain "original works of authorship," including computer software, literary works, musical works, and motion pictures. See 17 U.S.C. § 102(a). The interest in a using a commercial identity or brand to identify a product or service to consumers is protected federally by the law of trademark. 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.

New inventions, another kind of intellectual property, are often protected by obtaining a "patent," which is available for "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 gives the patentee the right to exclude others from making, using, and selling devices that embody the claimed invention. See 35 U.S.C. § 271(a). Patents protect products and processes, not pure ideas. Thus, Albert Einstein could not have received a patent for his novel ideas on the theory of relativity, but methods for using this theory in a nuclear power plant are patentable. Proposals for patenting genetic sequences or business methods are generally thought to be

pushing the limits of patent law.

Another way to use the law to protect a new invention is to treat it as a trade secret. In general, a trade secret is any formula, pattern, device or compilation of information used in a business to obtain an advantage over competitors who do not know or use it. Perhaps the most famous trade secret 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).

Personally identifiable information is another kind of intangible property that is increasingly becoming subject to control as a result of new legal regimes. A few narrow categories of information have been protected by federal law. See, e.g., Fair Credit Reporting Act, 15 U.S.C. § 1681 (consumer credit information). With the increased use of the Internet to trade in information, the public has expressed keen interest in controlling personally identifiable information. Congress and federal agencies have responded to that concern with laws protecting additional categories of information. See, e.g., Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 (1999) (to be codified at 45 C.F.R. pts. 160-164) (individually identifiable health information); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (personally identifiable information about children).

B. How Can Intellectual Property Be Misappropriated?

Intellectual property may be misappropriated in many ways. A copyrighted work may be illegally infringed by making and selling an unauthorized copy, as with pirated computer software. A trademark may be infringed by selling a good with a counterfeit mark. A person can infringe a patent by manufacturing and selling a product that functions according to the patent's description. A trade secret may be misappropriated by removing it from the possession of its owner and making use of it on behalf of a competitor.

Such misappropriation is not merely theoretical – it is flourishing. In fact, in 1996, Congress found that counterfeiting of trademark and copyrighted merchandise "is a multibillion-dollar drain on the United States economy" that "deprives legitimate trademark and copyright owners of substantial revenues and consumer goodwill" and "poses health and safety threats to United States consumers." See Anticounterfeiting Consumer Protection Act of 1996, Pub. L. No. 104-153, § 2, 110 Stat. 1386 (1996). In one recent Congressional report, it was noted that:

> Industry groups estimate that counterfeiting and piracy of intellectual property – especially computer software, compact discs, and movies – cost the affected copyright holders more than $11 billion last year [i.e., 1996] (others believe the figure is closer to $20 billion). In some countries, software piracy rates are as high as 90% of all sales. The U.S. rate is far lower (27%), but the dollar losses ($2.3 billion) are the highest worldwide.

> The effect of this volume of theft is substantial: 130,000 lost U.S. jobs, $5.6 billion in corresponding lost wages, $1 billion in lower tax revenue, and higher prices for honest purchasers of copyrighted software.

H.R. Rep. No. 105-339, at 4 (1997). Moreover, a 1988 National Institute of Justice study of trade secret theft in high technology industries found that 48 percent of 150 research and development companies surveyed had been the victims of trade secrets theft. Lois F. Mock & Dennis Rosenbaum, A Study of Trade Secret Theft in High-Technology Industries (May 1988) (unpublished manuscript on file with the National Institute of Justice). Accord S. Rep. No. 104-359, at 8 (1996).

C. What Intellectual Property Misappropriation Constitutes a Crime?

Although civil remedies that may provide compensation to wronged intellectual property rights holders are available, criminal sanctions are often warranted to ensure sufficient punishment and deterrence of wrongful activity. Indeed, because violations of intellectual property rights often involve no loss of tangible assets and, for infringement crimes, do not even require any direct contact with the rights holder, the rights holder often does not know it is a victim until a defendant's activities are specifically identified and investigated.

Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights specifically to ensure that those violations are not merely a cost of doing business for defendants. Among the most significant provisions are the following:

- The counterfeit trademark crime is set out at 18 U.S.C. § 2320
- Criminal infringement of copyrighted works is set out at 17 U.S.C. § 506(a) and 18 U.S.C. § 2319
- The counterfeit labeling provision is set out at 18 U.S.C. § 2318
- Theft of trade secrets prohibited by 18 U.S.C. §§ 1831 and 1832

Experience has proven that federal investigators and prosecutors can bring cases under these provisions that result in punishment for the wrongdoer, as well as deterrence for intellectual property crimes.

In addition, Congress is concerned about providing adequate protections for both foreign and domestic owners of intellectual property. Indeed, the United States government has committed, in a number of international agreements, to protect intellectual property rights holders, including foreign rights holders, from infringement in the United States. The United States is a member of the World Intellectual Property Organization ("WIPO") and the World Trade Organization ("WTO"), both of which administer agreements that have established international IP standards. The WTO's Agreement on Trade Related Aspects of Intellectual Property Rights ("TRIPS"), Sept. 27, 1994, is the most comprehensive agreement to date, and the first to include enforcement provisions.

Some misuse of intellectual property has not been criminalized. For example, infringement of a patent is not generally a criminal violation. Likewise, the laws protecting personally identifiable information do not generally provide for criminal penalties except in the most narrow of circumstances. See 18 U.S.C. § 2710 (wrongful disclosure of video tape rental or sale records).

D. Enforcement of Intellectual Property Laws and the First Amendment

Enforcement of intellectual property laws in America can sometimes be at tension with the constraints of the First Amendment. This strain has long been recognized both in copyright and trademark law. See, e.g., Paul Goldstein, Copyright and the First Amendment, 70 Colum. L. Rev. 983 (1970); Robert N. Kravitz, Trademarks, Speech, and the Gay Olympics Case, 69 B.U. L. Rev. 131 (1989); Arlen W. Langvardt, Protected Marks and Protected Speech: Establishing the First Amendment Boundaries in Trademark Parody Cases, 36 Vill. L. Rev. 1 (1991); Melville B. Nimmer, Does Copyright Abridge the First Amendment Guarantees of Free Speech and Press?, 17 UCLA L. Rev. 1180 (1970). New technologies such as the Internet provide fertile ground for revisiting these conflicts. See, e.g., Christopher E. Gatewood, Click Here: Web Links, Trademarks and the First Amendment, 5 Richmond J.L. & Tech. 12 (1999); John Gladstone Mills III, Entertainment on the Internet: First Amendment and Copyright Issues, 79 J. Pat. & Trademark Off. Soc'y 461 (1997).

Moreover, growth of intellectual property law is also subject to constitutional limit. Indeed, as one scholar has observed, "[r]ecent expansions of intellectual property law have put more strain on the uneasy truce between" intellectual property law and the First Amendment. Mark A. Lemley, The Constitutionalization of Technology Law, 15 Berkeley Tech. L.J. 529, 530-31 (2000). Prosecutors should be aware of the potential constitutional limitations (particularly First Amendment limitations) when charging cases under novel theories of intellectual property law. Cf. Yochai Benkler, Constitutional Bounds of Database Protection: The Role of Judicial Review in the Creation and Definition of Private Rights in Information, 15 Berkeley Tech. L.J. 535 (2000).

E. The Intellectual Property Rights Initiative

On July 23, 1999, The Department of Justice, the Federal Bureau of Investigation, and the U.S. Customs Service announced the establishment of a law enforcement initiative aimed at combating the growing challenge of piracy and counterfeiting of intellectual property, both domestically and internationally. Domestically, United States Attorneys, the Federal Bureau of Investigation, and the Customs Service agreed to increase their enforcement efforts nationwide, with particular emphasis in seven target districts. Internationally, the initiative pledges support from the Justice Department, including the FBI, for existing efforts of the State Department, Customs Service, and trade agencies with specialized expertise in intellectual property issues – the U.S. Trade Representative, the Department of Commerce's Patent & Trademark Office, and the Copyright Office – to enhance their technical assistance capabilities and training priorities.

Key components of the Intellectual Property Rights Initiative include:

- Increasing the priority of criminal IP investigations and prosecutions nationwide, beginning with the targeted districts;
- Increasing specialized training courses for investigators and prosecutors;
- Developing training programs for state and local officials;
- Seeking referrals from industry through a streamlined system;
- Utilizing procedures for forfeiture of infringing merchandise as an additional tool to get illegal products off the streets;
- Continuing efforts to increase criminal penalties for infringement by amending the Sentencing Guidelines;
- Highlighting U.S. trade priorities in international law enforcement anti-piracy efforts, including the prioritization of key countries for U.S. training and technical assistance.

The Intellectual Property Initiative was announced by Deputy Attorney General Eric H. Holder, Jr., announced the initiative in San Jose, Cal., along with FBI Assistant Director, Criminal Investigative Division, Thomas J. Pickard; Sam Banks, Deputy Commissioner of the U.S. Customs Service; United States Attorney Robert S. Mueller, III from the Northern District of California; and United States Attorney Alejandro Mayorkas from the Central District of California. For Deputy Attorney General Holder's remarks, see <http://www.cybercrime.gov/dagipini.html>.

II. TRAFFICKING IN COUNTERFEIT GOODS OR SERVICES: 18 U.S.C. § 2320

Trademarks and service marks are part of the fabric of American society today. Americans rely on the brands they represent when purchasing and using all manner of goods and services. This reliance gives companies an incentive to maintain quality control over the goods they produce and mark. In addition, companies that sell quality goods invest heavily in their brand. For example, they pay top dollar to sponsor sporting events, sporting arenas, and have celebrities endorse them.

Black's Law Dictionary defines "trademark" as "a distinctive mark of authenticity, through which the products of particular manufacturers or the vendible commodities of particular merchants may be distinguished from those of others." Black's Law Dictionary 1493 (6th ed. 1990). The Lanham Act, which was enacted in 1946 as part of a comprehensive revision of civil trademark law and the trademark registration process, defines "trademark" to include "any word, name, symbol, or device, or any combination thereof – (1) used by a person, or (2) which a person has a bona fide intention to use in commerce and applies to register on the principal register established by [the Lanham Act], 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, even if that source is unknown." 15 U.S.C. § 1127. Among the most widely recognized trademarks are "Kodak" for photography equipment and the Nike "swoosh" for sports apparel. Service marks identify distinctive features of services, such as athletic events or television shows, rather than goods. See 15 U.S.C. § 1127. For simplicity, this manual usually refers to trademarks and sales of goods rather than service marks and selling of services, although the legal analysis is the same.

Commercial trademarks are the currency of modern commerce. This chapter first discusses the functions protected by trademark, then discusses the trademark counterfeiting statute, elements of the crime, defenses to the crime, and penalties imposed by the statute. Finally, this chapter discusses cases where the counterfeit goods are arguably of comparable quality to the legitimate goods, and it provides a case study in a cutting edge context: trafficking in remarked computer chips as a counterfeiting crime. Forms providing sample indictments and jury instructions for trademark counterfeiting, 18 U.S.C. § 2320, are provided in Appendix B at page 165. Prosecutors may find other resources to be helpful as well, including treatises, see, e.g., J. Thomas McCarthy, McCarthy on Trademarks and Unfair Competition (1995). Law review articles may also be of assistance. See, e.g., Michael Coblenz, Intellectual Property Crimes, 9 Alb. L.J. Sci. & Tech. 235 (1999); Randy Gidseg et al., Intellectual Property Crimes, 36 Am. Crm. L. Rev. 835 (1999); David J. Goldstone & Peter J. Toren, The Criminalization of Trademark Counterfeiting, 31 Conn. L. Rev. 1 (1998).

A. Functions Protected by Trademark

One commentator has observed that courts recognize and protect four functions performed by trademarks. These are: (1) identifying a particular seller's goods and

distinguishing them from goods sold by others; (2) signifying that all goods bearing the trademark come from or are controlled by a single source; (3) signifying that all goods bearing the trademark are of an equal level of quality; and (4) serving as a prime instrument in advertisement and sale of the goods. 1 J. Thomas McCarthy, McCarthy on Trademarks and Unfair Competition § 3.01[2] (1995). A trademark is also 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.[1]

Ownership of a mark arises not through any single act of federal registration, but rather through continued use. Under its power to regulate interstate commerce, Congress has established a federal administrative process for registering trademarks. This process coexists with state common-law trademark rights. However, registration of a mark with the Patent and Trademark Office offers many legal advantages, including – procedurally – access to the federal courts under 15 U.S.C. § 1121, and – substantively – the possibility of recovery of lost profits, damages, and costs, and the availability of treble damages and attorney fees. See 15 U.S.C. § 1117.

Most importantly for prosecutors, federal registration is a jurisdictional prerequisite to federal criminal prosecution and is an essential element in a prosecution for trademark counterfeiting, since the government must show that the genuine mark was registered on the principal register in the United States Patent and Trademark Office in order to establish the existence of the "counterfeit" mark. See 18 U.S.C. § 2320(e)(1)(A)(ii). To register a trademark on the principal register, the owner must establish (1) distinctiveness of the mark, and (2) use or intent to use the mark in interstate or foreign commerce. See 15 U.S.C. § 1052.

Although trademark law has been primarily part of civil rather than criminal practice, Congress had important reasons and ample precedent for criminalizing trademark counterfeiting when it did so in 1984. Indeed, criminal trademark law dates back to at least 1541, when an English statute prohibited obtaining another's property by means of a "false Token or counterfeit Letter made in any other Man's Name." 33 Hen. VIII, c.1 (1541), cited in 2 William R. Lafave & Austin W. Scott, Jr., Substantive Criminal Law § 8.7, at 383 n.2 (1986). The criminalization of

---

[1] Prosecutors unfamiliar with trademark law may be more familiar with anti-counterfeiting laws designed to protect traditional national currencies and national symbols. The purpose of trademark law is similar to the purposes of these laws. See, e.g., 18 U.S.C. §§ 471-474 (counterfeiting activities relating to obligations or securities of the United States), 478-481 (counterfeiting activities relating to foreign obligations or securities), 501 (counterfeiting postage stamps), 506 (counterfeiting seals of departments or agencies), 706 (Red Cross emblem), 707 (4-H club emblem), 708 (Swiss Confederation coat of arms), 709 (false advertising or misuse of names to indicate federal agency), 711-715 (national symbols, including seals of the United States, Golden Eagle insignia, and Smokey Bear character or name), 1159 (misrepresentation of Indian produced goods and products).

trademark counterfeiting serves at least four important functions:

(1) Protecting the intellectual property assets of a trademark holder from theft or dilution. A counterfeiter should be no more able to steal a company's good name (and profit stream associated with that name) than a company's profits. Trademark holders cannot protect their intellectual property through the traditional security means – such as guards and audits – used to protect their other assets. Also, by selling inferior products, the counterfeiter devalues a trademark holder's good name even while profiting from it.

(2) Protecting consumers from fraud. Consumers are entitled to rely on trademarks when making their purchasing decisions. Yet counterfeit goods can be of much lower quality, and can even present serious health or safety risks to consumers, as in the cases of counterfeit food products, prescription drugs, or automotive parts. Trademark counterfeiting can be an especially pernicious kind of fraud because counterfeit goods are often distributed widely through layers of intermediaries. With dispersed victims and small losses per victim, a large-scale counterfeiter can often evade civil and criminal sanctions.

(3) Protecting safety in society for non-purchasing users. Sales of counterfeit products often victimize not only the trademark holder and purchaser, but also non-purchasing users. For example, airlines may purchase counterfeit airplane parts of which passengers may be victims; hospitals may purchase counterfeit heart pumps of which patients may be victims; and parents may purchase counterfeit infant formula that harms their children. These examples and others are provided in H.R. Rep. No. 104-556, at 3 (1996), reprinted in 1996 U.S.C.C.A.N. 1074, 1076, and S. Rep. No. 98-526, at 4 (1984), reprinted in 1984 U.S.C.C.A.N. 3627, 3630.

(4) Enforcing market rules. Just as counterfeiting money and forgery are crimes that undermine fundamental market rules, counterfeiting of trademarks weakens modern commercial systems.

B. The Trademark Counterfeiting Crime and Its Elements

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

> 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 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.

In order to establish a criminal offense under 18 U.S.C. § 2320, courts have required the government to prove four elements of which two (the second and fourth elements) are mens rea elements:

(1) the defendant "trafficked" or attempted to traffic in goods or services;

(2) such trafficking, or the attempt to traffic, was "intentional";

(3) the defendant used a "counterfeit mark" on or in connection with such goods or services; and

(4) the defendant "knew" that the mark so used was counterfeit.

United States v. Giles, 213 F.3d 1247, 1249 (10th Cir. 2000) (reversing conviction for trafficking in counterfeit patches because statute does not prohibit trafficking in counterfeit labels unconnected to any goods); United States v. Sultan, 115 F.3d 321, 325 (5th Cir. 1997) (reversing conviction for trafficking in counterfeit automobile parts because proof was insufficient that defendant knew he was purchasing and selling counterfeit parts). Aiding and abetting or conspiring to violate the statute can be prosecuted in conjunction with 18 U.S.C. §§ 2 and 371. See United States v. Yamin, 868 F.2d 130 (5th Cir.) (affirming conviction for conspiracy and trafficking in counterfeit watches), cert. denied, 492 U.S. 924 (1989).

Three significant absences are worth noting. First, even though there are two knowledge elements under 18 U.S.C. § 2320, there is no requirement of "specific intent": Congress did not require proof of either an intent to defraud or an awareness that the defendant was violating a specific statute. See United States v. Gantos, 817 F.2d 41, 42-43 (8th Cir.) (affirming conviction on intent to traffic, rather than "specific intent" to violate a statute), cert. denied, 484 U.S. 860 (1987); United States v. Baker, 807 F.2d 427, 429-29 (5th Cir. 1986) (affirming conviction because defendant need not have known his conduct was a crime). Second, there is no requirement of loss by any particular victim. For example, it is not necessary to demonstrate that the product trafficked in is of lesser quality than the genuine product. Even if the consumer is not defrauded, the counterfeiter is still trading off the name of another without authorization. Third, the statute provides no minimum requirement of scale for the crime of trademark counterfeiting. In contrast to the criminal copyright law, even small scale counterfeiting constitutes a felony. Cf. 18 U.S.C. § 2319(b) (providing punishment for copyright infringement as a felony only if at least ten copies with a retail value of more than $2,500 were reproduced or distributed). Nevertheless, scale of infringement is relevant for sentencing in determining "loss" for purposes of the Guidelines. See infra Section VII.A at page 109 (discussing the sentencing guidelines for infringement crimes).

Clarifying 18 U.S.C. § 2320 by using civil trademark law. In interpreting the scope of the provisions of 18 U.S.C. § 2320, it can be helpful to consider sister provisions under the civil trademark law, which was codified in 1946 as the Lanham Act, 15 U.S.C. §§ 1051-1127, and has been the subject of numerous reported cases. This body of law can be particularly of use in interpreting provisions with similarities or definitions. Indeed, Lanham Act itself is defined in 18 U.S.C. § 2320(e)(3). The defenses to 18 U.S.C. § 2320 specifically incorporate the Lanham Act

defenses. See 18 U.S.C. § 2320(c). The legislative history refers repeatedly to the Lanham Act's body of case law as the background against which Congress intended the criminal prohibition to be interpreted. See, e.g., 130 Cong. Rec. 31,675 (1984) ("no conduct will be criminalized by this act that does not constitute trademark infringement under the Lanham Act") (Joint Statement on Trademark Counterfeiting Act).

The courts have taken the cue from Congress to adapt civil Lanham Act principles to criminal cases. For example, in United States v. Petrosian, the Ninth Circuit, in the absence of criminal precedent, affirmed the defendant's conviction by relying exclusively on two civil cases brought under the Lanham Act. 126 F.3d 1232 (9th Cir. 1997), cert. denied, 522 U.S. 1138 (1998). The court explained its resort to civil case law by noting that the "definition of the term 'counterfeit mark' in the Lanham Act is nearly identical to the definition in 18 U.S.C. § 2320, suggesting that Congress intended to criminalize all of the conduct for which an individual may be civilly liable." Id. at 1234. See also United States v. Torkington, 812 F.2d 1347, 1352 (11th Cir. 1987) (applying a standard drawn from the Lanham Act because "Congress . . . manifested its intent that 18 U.S.C. § 2320(d)(1)(A)(iii) be given the same interpretation as is given the identical language in 17 U.S.C. § 1114(1) of the Lanham Act") (citing H.R. Rep. No. 98-997, at 8, 12 (1984); 130 Cong. Rec. 31,675 (1984) (Joint Statement on Trademark Counterfeiting Act)). Nevertheless courts have not refrained from noting differences between the criminal and civil trademark statutes even while applying Lanham Act standards to criminal cases. See United States v. Hon, 904 F.2d 803, 806-07 (2d Cir. 1990) (enumerating differences between 18 U.S.C. § 2320 liability and Lanham Act liability but applying the standard from the Lanham Act), cert. denied, 498 U.S. 1069 (1991); United States v. Torkington, 812 F.2d 1347, 1350 (11th Cir. 1987) (noting that 18 U.S.C. § 2320 is "narrower in scope" than the Lanham Act).

1. "Trafficked" in goods or services

The first element, to "traffic" in goods or services, is defined broadly 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." This definition is broad enough to cover all aspects of commercial activity from initial manufacture to sale to ultimate purchasers. The thing "of value" received as consideration need not be a financial payment. See United States v. Koehler, 24 F.3d 867, 870-71 (6th Cir. 1994) (affirming conviction based on acceptance of air conditioner compressors in lieu of financial payment), cert. denied, 513 U.S. 1077 (1995). However, the knowing "purchase" of goods bearing counterfeit marks for personal use was not intended to be covered by 18 U.S.C. § 2320. See Joint Statement on Trademark Counterfeiting Legislation, 130 Cong. Rec. 31,675 (1984) (hereinafter "Joint Statement").

2. Trafficking was "intentional"

The first of two mens rea elements is that the defendant's trafficking was "intentional"; that is, that he or she acted deliberately or "on purpose." See, e.g., Baker, 807 F.2d at 428-30

(affirming conviction for trafficking on the basis of intent to traffic rather than knowledge of crime); see also United States v. Hon, 904 F.2d 803, 806 (2d Cir.) (affirming conviction for trafficking and attempting to traffic in counterfeit wristwatches), cert. denied, 498 U.S. 1069 (1991); Joint Statement, 130 Cong. Rec. 31,674 (1984). As noted above, however, the statute does not require a specific intent to violate the statute. See supra Section II.B at page 17.

3. The defendant used a "counterfeit mark" on or in connection with goods or services

The third element of the crime of trademark counterfeiting is that the defendant used a "counterfeit mark" on or in connection with goods or services. The statute requires some nexus between the "mark" and the "goods or services" sufficient to describe the connection as a "use." This requirement is essentially duplicated within the definition of the term "counterfeit mark" and is discussed below. The term "counterfeit mark" is a term of art, and is defined by 18 U.S.C. § 2320(e)(1)(A)[2] as follows:

> (A) a spurious mark—
>
> (i) that is used in connection with trafficking in goods or services;
>
> (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; and
>
> (iii) the use of which is likely to cause confusion, to cause mistake, or to deceive.

Although by its terms 18 U.S.C. § 2320 seems to require that the "mark" be counterfeit (rather than, for example, requiring that the goods be counterfeit), the courts have not been unduly concerned with this technicality where the trademark holder is deprived of the ability to control the quality of products bearing its name and where consumer confusion is likely, so long as the other formalities have been met. For example, the defendant in United States v. Petrosian purchased "genuine Coca-Cola bottles," filled them with a cola-like carbonated beverage that was not Coca-Cola, and told purchasers that the beverage was Coca-Cola. 126 F.3d 1232 (9th Cir. 1997), cert. denied, 522 U.S. 1138 (1998). The Ninth Circuit rejected the defendant's contention that the use of the Coca-Cola mark could not be counterfeit because it was a "genuine" mark, and observed 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

---

[2] 18 U.S.C. § 2320(e)(1)(B) incorporates into the definition trademarks protected by the Olympic Charter Act.

of the beverage in the bottles and falsely identified the beverage in the bottles as Coca-Cola." Id. at 1234. The importance of a mark holder being able to control the quality of goods associated with its mark is discussed further below with regard to cases of "comparable" goods. See infra Section II.E at page 27.

The statute itself requires that the "use" of the counterfeit mark be "likely to cause confusion, to cause mistake, or to deceive." 18 U.S.C. § 2320(e)(1)(A)(iii). In interpreting this provision, courts have held that "[t]he jury need not find actual confusion." United States v. Yamin, 868 F.2d 130, 133 (5th Cir.) (affirming conviction for conspiracy and trafficking in counterfeit watches), cert. denied, 492 U.S. 924 (1989). Instead, they consistently have employed an objective standard. "The statute expressly requires only likelihood of confusion." Id. Accord United States v. Hon, 904 F.2d 803, 806-08 (2d Cir.) (approving jury consideration of likelihood of confusion in addition to actual confusion), cert. denied, 498 U.S. 1069 (1991); United States v. Torkington, 812 F.2d 1347, 1350-52 (11th Cir. 1987) (holding that confusion of direct purchasers is unnecessary, if the purchasing public is likely to be confused). Because subsequent purchasers or recipients of the goods may be duped and because of the need to protect the trademark owner's investment in the quality of the mark and its product's reputation, it is not a defense that the original buyer was told that the goods were counterfeit, or that the buyer was actually not confused for other reasons, e.g., because of the comparatively low price of the fake goods. See Hon, 904 F.2d at 806-08; Torkington, 812 F.2d at 1350-52; United States v. Gantos, 817 F.2d 41, 43 (8th Cir.) (rejecting defendant's argument that revelation to purchaser that goods were counterfeit exonerates him), cert. denied, 484 U.S. 860 (1987). The trier of fact may decide whether the possibility of confusion is likely either through a side-by-side comparison of products, through expert testimony, or both. Yamin, 868 F.2d at 133; United States v. DeFreitas, 92 F. Supp.2d 272, 278 (S.D.N.Y. 2000) (noting that "the jury was free to compare the tags and the marks on the genuine and on the counterfeit Beanie Babies").

The "likelihood of confusion" standard is taken from the Lanham Act, 15 U.S.C. § 1114(1). According to the legislative history, this phraseology was chosen to ensure that "no conduct [would] be criminalized. . .that does not constitute trademark infringement under the Lanham Act." 130 Cong. Rec. 31,675 (1984). Thus, in reviewing the sufficiency of the evidence for purposes of deciding a motion to dismiss an indictment, courts have employed the same factors used in civil proceedings to analyze whether there is a likelihood of confusion between two marks. See Torkington, 812 F.2d at 1352. These factors have included: (1) the type of trademark; (2) the similarity of design; (3) the similarity of product; (4) the identity of retailers and purchasers; (5) the similarity of advertising media used; (6) the defendant's intent; and (7) any actual confusion. Id. at 1354. See United States v. McEvoy, 820 F.2d 1170, 1172 (11th Cir. 1987); see also Polaroid Corp. v. Polarad Elecs.. Corp., 287 F.2d 492, 495 (2d Cir.) (enumerating so-called Polaroid factors: "the strength of [plaintiff's] mark, the degree of similarity between the two marks, the proximity of the products, the likelihood that the prior owner will bridge the gap, actual confusion, and the reciprocal of defendant's good faith in adopting its own mark, the quality of defendant's product, and the sophistication of the buyers"), cert. denied, 368 U.S. 820 (1961).

The registration and the "in use" requirements are not usually contested although they are important technical requirements. The statute requires that genuine mark is "registered" on the "principal register" in the United States Patent and Trademark Office. 18 U.S.C. § 2320(e)(1)(A)(ii). Federal registration is a jurisdictional prerequisite to federal criminal prosecution and is an essential element in a prosecution for trademark counterfeiting. See United States v. DeFreitas, 92 F. Supp.2d 272, 278 (S.D.N.Y. 2000) (finding testimony of mark holder for Beanie Babies along with samples of genuine, marked Beanie Babies and the mark holder's catalog to be sufficient evidence to permit a jury to conclude that the mark was registered).[3] Often a prosecutor may prove this element simply by offering a certified copy of the registration, which can be obtained from the U.S. Patent and Trademark Office. See Appendix A at page 159 (intellectual property contact lists).

The registration of a trademark by the Federal Patent and Trademark Office establishes a statutory presumption of ownership of the trademark and the validity of the registration. 15 U.S.C. § 1057(b) ("A certificate of registration of a mark upon the principal register . . . shall be prima facie evidence of the validity of the registered mark . . . of the registrant's ownership of the mark, and of the registrant's exclusive right to use the registered mark in commerce or in connection with the goods or services specified in the certificate . . . ."). Indeed, experience with prosecutions brought under the statute is that the genuine mark is treated as "incontestible" because 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"). Such well-established marks probably provide the most appealing marks for counterfeiters to misappropriate. Although the government must prove the mark was so registered, the statute explicitly states that the government need not prove the defendant's awareness of that registration. See 18 U.S.C. § 2320(e)(1)(A)(ii).

Another requirement is that the genuine mark be "in use." 18 U.S.C. § 2320(e)(1)(A)(ii). No further definition is provided in the statute, the case law, or the legislative history. Although this requirement is not normally in dispute, some guidance might be drawn from the Lanham Act registration prerequisite that the mark be "use[d] in commerce," which is defined broadly 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 ConAgra, Inc. v. George A. Hormel & Co., 990 F.2d 368, 371-72 (8th Cir. 1993) (affirming district's finding that Hormel's trademark application was not based on a "sham use").

The legislative history provides some commentary on other parts of the statute's definition of "counterfeit mark." Where the statute requires the mark to be "spurious," 18 U.S.C. § 2320(e)(1)(A), the legislative history states that "spurious" means "not genuine or authentic." 130 Cong. Rec. 31,675 (1984). Where the statute requires that the counterfeit mark be "identical

---

[3] To register a trademark on the principal register, the owner must establish (1) distinctiveness of the mark, and (2) use or intent to use the mark in interstate or foreign commerce. See 15 U.S.C. § 1052.

with, or substantially indistinguishable from" a genuine trademark, 18 U.S.C. § 2320(e)(1)(A)(ii), the legislative history states that the phrase "substantially indistinguishable from" is intended to prevent a counterfeiter from escaping liability by modifying a protected trademark in trivial ways. Conversely, it also serves to exclude the arguable case of trademark infringement that is merely "reminiscent of" protected trademarks. 130 Cong. Rec. 31,675-76 (1984). Incidentally, this standard is the same as that applied in civil actions under the Lanham Act. See 15 U.S.C. § 1127 (defining "counterfeit" as a spurious mark which is "identical with, or substantially indistinguishable from, a registered mark").

Finally, the statute restricts the "goods or services" with which the mark is "used" to be "those goods or services" for which the genuine mark is registered. 18 U.S.C. § 2320(e)(1)(A)(i)-(ii). This restriction is an important distinction from civil trademark infringement under the Lanham Act. As the legislative history notes, "a plaintiff with a Federal registration for. . .[a mark] on typewriters might have a 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.'" 130 Cong. Rec. 31,676 (1984). One other consequence of this restriction is that knowing trafficking in unattached counterfeit marks would not by itself fulfill the requirements of the statute. United States v. Giles, 213 F.3d 1247, 1253 (10th Cir. 2000) (reversing conviction for trafficking in counterfeit patches because statute does not prohibit trafficking in counterfeit labels unconnected to any goods). Nevertheless, it could expose a defendant to liability as an aider and abetter in trademark counterfeiting. Id. at 1251 n.6. By contrast, trafficking in counterfeit labels for copyrighted works can be subject to criminal penalties under 18 U.S.C. § 2318 even if the labels are not attached to a work. See infra Section IV.A.2 at page 67.

4. The defendant "knowingly used" the counterfeit mark

The fourth element of the crime of trademark counterfeiting is that the defendant "knowingly" used the counterfeit mark on or in connection with the trafficked goods or services. The requisite showing of knowledge, or willful blindness, may be made through direct or circumstantial evidence. The Seventh Circuit, in an opinion by Judge Easterbrook, noted that the defendant "knew that the marks were on the bottles, caps and boxes," and found this knowledge to be sufficient to uphold a conviction. United States v. Sung, 51 F.3d 92, 93 (7th Cir. 1995) (holding that the vendor is on duty to inquire into the status of a mark). Typical circumstantial evidence includes, but is not limited to, evidence of a defendant's purchase or sale of the goods, manipulation of the goods, the method of delivery, packaging conventions, or an unusually low price. Indeed, the profits and circumstantial evidence regarding knowledge are usually so overwhelming that this element is not often contested. See, e.g., United States v. McEvoy, 820 F.2d 1170, 1173 (11th Cir.) ("It is telling that the trial record reveals that appellants were very much aware that their actions in selling the watches violated the law."), cert. denied, 484 U.S. 902 (1987). On the other hand, the Fifth Circuit has held that the government failed to satisfy the "knowingly" requirement where the accused trafficker in counterfeit goods did not affix the mark

himself and where the government had not shown he knew that the mark was in fact being affixed to it by the counterfeiter. United States v. Sultan, 115 F.3d 321, 325-30 (5th Cir. 1997) (reversing conviction for trafficking in counterfeit automobile parts).

The legislative history clarifies that the drafters intended that the government should prove that the defendant had "an awareness or a firm belief to that effect." 130 Cong. Rec. 31,674 (1984) (referring to an awareness or belief to the effect that the mark was counterfeit). This mens rea is notably different from (and less burdensome to prove than) an "intentional" mental state, as is required by the second element of the crime. For example, the legislative history states that "if 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.'" 130 Cong. Rec. 31,674 (1984) (citing United States v. Jewell, 532 F.2d 697 (9th Cir.), cert. denied, 426 U.S. 951 (1976)). On the other hand, the Congressional sponsors believed that "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." 130 Cong. Rec. 31,674 (1984).[4]

There are a number of aspects of knowledge that do not have to be shown by the government. First, the government does not have to show that the defendant knew that a mark was registered for those goods or services on the principal register, because the statute itself states that the definition of counterfeit mark applies "whether or not the defendant knew such mark was so registered." 18 U.S.C. § 2320(e)(1)(A)(ii). See Sung, 51 F.3d at 94. Second, just as the government need not show actual confusion, it is not required to prove an intent to mislead. 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"). Finally, lack of knowledge of the criminality of the conduct is not an element of the offense. As previously discussed, the crime does not require a specific intent to violate the statute.

C. Defenses to the Crime of Trademark Counterfeiting

Overrun and "grey market" goods. The statute expressly excludes from the definition of "counterfeit mark" any mark used in connection with items (commonly termed "overrun goods") that are:

> 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

---

[4] Care must be exercised when offering the so-called "conscious avoidance" or "ostrich" instruction first set forth in United States v. Jewell, 532 F.2d 697 (9th Cir.) (en banc), cert. denied, 426 U.S. 951 (1976). There are significant differences throughout the circuits regarding the appropriateness of such an instruction and the precise language to be used. Prosecutors should consult local circuit opinion on this matter prior to proceeding with a Jewell instruction.

> 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).

The legislative history makes clear that "overrun goods" is an affirmative defense, and that "the burden will be on the defendant to prove that the goods or services in question fall within the overrun exclusion, under both the criminal and civil provisions." 130 Cong. Rec. 31,676 (1984). The First Circuit rejected a defendant's vagueness challenge to the overrun exclusion, and held instead, based on the plain language of the statute, that Congress intended the exception to be limited to those 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, 579-81 (1st Cir. 1995) (affirming conviction for trafficking in counterfeit goods and importing goods by means of false or fraudulent practices).

The legislative history provides an example: If a licensee was authorized to make 500,000 umbrellas bearing a trademark owner's mark and the licensee manufactured without authorization an additional 500,000 umbrellas bearing that mark during the course of the license, "the contractual and other civil remedies already existing make it inappropriate to criminalize such practices." 130 Cong. Rec. 31,676 (1984) (citation omitted). On the other hand, the legislative history also explains that the exclusion cannot be claimed where a licensee produces a type of good other than the one for which he or she is licensed. For example, "if a licensee is authorized to produce 'Zephyr' trench coats, but without permission manufactures 'Zephyr' wallets, the overrun exception would not apply." 130 Cong. Rec. 31,677 (1984).

Also excluded from the definition of counterfeit mark are so-called "parallel imports" or "gray market" goods, which are trademarked goods legitimately manufactured and sold overseas, and then imported into the United States outside of the trademark owner's traditional distribution channels. The mark placed on the gray market goods is not considered counterfeit under the statute because it was placed there with the consent of the trademark owner, and the goods were not subsequently modified or remarked. Congress carefully considered "gray market" goods, and intended that they fall outside of the statute. 130 Cong. Rec. 31,676 (1984); S. Rep. No. 98-526, at 11 (1984), reprinted in 1984 U.S.C.C.A.N. 3627, 3637.

Lanham Act defenses. 18 U.S.C. § 2320(c) explicitly incorporates all the civil Lanham Act defenses into the criminal cases: "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." In considering this provision, the legislative history notes that "only those defenses, affirmative defenses, and limitations on relief that are relevant under the circumstances will be applicable. . ." 130 Cong. Rec. 31,675 (1984). The legislative history confirms Congress' intent that "any affirmative defense under the Lanham Act will remain an affirmative defense under this Act." Id.

Lanham Act defenses in cases involving so-called "incontestible marks," which are the most commonly counterfeited and thus provide the basis for most criminal prosecutions, are primarily set out at 15 U.S.C. § 1115(b). These nine defenses are enumerated as follows: (1) fraud by the mark owner in obtaining the registration; (2) abandonment of the mark by its owner; (3) misrepresentation or unclean hands with respect to use of the mark; (4) fair use; (5) innocent prior use without registration; (6) innocent prior use with registration; (7) use of a trademark in violation of the antitrust laws; (8) use of a functional mark; and (9) equitable defenses, such as laches, estoppel, and acquiescence. Other Lanham Act defenses or limitations prominently mentioned in the legislative history are those limitations on actions against printers and newspapers in 15 U.S.C. § 1114(2). See 130 Cong. Rec. 31,675 (1984). For an extensive discussion of each of these defenses, see David J. Goldstone & Peter J. Toren, The Criminalization of Trademark Counterfeiting, 31 Conn. L. Rev. 1, 43-65 (1998).

Where such defenses are raised, case law under the Lanham Act, 15 U.S.C. §§ 1051-1127, may prove instructive, although they can not be applied mechanically to a criminal case. For example, an "unclean hands defense" may be used to deny relief to an "unclean" plaintiff mark holder in a civil case. 15 U.S.C. § 1115(b)(3). However, the wrongful activity of a purportedly "unclean" mark holder may be less relevant to a criminal case, where the mark holder is not actually a party. In a criminal case, prosecutors act in the interest of the public, not just the victim mark holder. Permitting the defendant to automatically avail itself of this Lanham Act defense may not vindicate the public interest.

General defenses. Many general defenses to 18 U.S.C. § 2320 arise outside the statute, such as the running of the statute of limitations, the absence of proper venue, or the absence of proper jurisdiction. These defenses are available in every criminal case and their application needs no further elaboration here. However, the statute of limitations defense for violations of 18 U.S.C. § 2320 merits additional discussion because of a law journal article suggesting that the statute of limitations for a 18 U.S.C. § 2320 violation should not be the usual five-year period as for almost all non-capital federal crimes under 18 U.S.C. § 3282, see, e.g., United States v. Milstein, No. CR 96-899 (RJD), 2000 WL 516784, at *3 (E.D.N.Y. March 3, 2000) (recognizing appropriateness of five-year statute of limitations), but should be based on the applicable period for civil trademark infringement in whichever state the federal court sits. See Ronald J. Nessim, Criminal (and Civil) Trademark Infringement: What Statute of Limitations Applies?, 76 J. Pat. & Trademark Off. Soc'y 933 (1994). Nessim's theory would encourage forum shopping in trademark cases and make statute of limitations analysis much less predictable. It has been raised by defense counsel in a number of litigated cases, but has not been adopted by any court of which we are aware. Because no special limitations period is "expressly provided for by law" in 18 U.S.C. § 2320, the five-year limitations period set out in 18 U.S.C. § 3282 is the proper one to use. See David J. Goldstone & Peter J. Toren, The Criminalization of Trademark Counterfeiting, 31 Conn. L. Rev. 1, 65-70 (1998) (arguing that federal courts should follow 18 U.S.C. § 3282 in cases arising under 18 U.S.C. § 2320).

D. Statutory Penalty for Trafficking in Counterfeit Goods or Services

The maximum penalty for violating 18 U.S.C. § 2320 is imprisonment for 10 years and a fine of $2,000,000 for a first-time violator. 18 U.S.C. § 2320(a). A subsequent conviction carries a prison term of up to 20 years, a $5,000,000 fine, or both. Id. For a first-time corporate defendant, the maximum fine is $5,000,000; recidivist corporations may be fined up to $15,000,000. Id. The defendant is sentenced under U.S. Sentencing Commission, Guidelines Manual § 2B5.3 (Nov. 1998 & Supp. 2000) (hereinafter U.S.S.G.). For detailed discussion of consequences of a conviction under 18 U.S.C. § 2320, see Chapter VII at page 108.

E. Counterfeit Goods That Are Comparable To Legitimate Goods

Cases involving trafficking in marked goods that are comparable to legitimate goods can seem to raise slightly different issues than so-called "ordinary" counterfeit goods cases. The majority of counterfeit goods cases involve counterfeit marks placed on goods that are substantially different from and usually of markedly lower quality than legitimate goods. In a garden-variety counterfeiting case, a counterfeiter might place on low-quality watches a counterfeit mark that is legitimately placed on watches that sell for over $1,000. By contrast, in a comparable goods case, the defendant might place the mark on similar-quality watches – perhaps on watches made by the same third-party manufacturer as is ordinarily used by the mark holder. These "comparable goods" cases are discussed below, with special attention given to computer chip ("CPU") remarking cases.

1. Background on comparable goods cases generally

A comparable goods case is one where the counterfeit mark is placed on goods where the goods themselves are arguably of equivalent quality to legitimate goods. For example, a defendant who is charged with trademark counterfeiting for selling pirated computer software in counterfeit packaging may claim that the software he sold was an exact duplicate of the original software. Therefore, he might claim, his use of the mark was justified, or at least should be excused.

These cases have arisen in many contexts, ranging from baby food to pharmaceuticals to physical goods to computer chips. See, e.g., United States v. Milstein, No. CR 96-899 (RJD), 2000 WL 516784, at *3 (E.D.N.Y. March 3, 2000) (pharmaceuticals). See also, e.g., United States Attorney's Office, Northern District of Texas, Federal Jury Convicts Four Individuals on Charges of Trademark Counterfeit, Conspiracy for Reselling Infant Formula, July 18, 2000 <http://www.cybercrime.gov/babyfood.htm>; 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 <http://www.cybercrime.gov/platinum.htm>; Department of Justice, Violation of I.B.M. Trademark Results in $3.3 Million Fine and Restitution for Chicago-area Company, November 19, 1998 <http://www.cybercrime.gov/desktop.htm>.

Defendants typically purchase loose goods at a low price – either government surplus,

goods that turn out to have been stolen, unmarked goods from an original equipment manufacturer ("OEM") or simply goods of only slightly lower quality – and then mark them or box them for sale at full price. Indeed, the practice by a mark holder of using OEMs to manufacture goods to be marked by the mark holder may permit a defendant to claim that his counterfeit goods were identical to the mark holder's because all goods made by a particular OEM are of the same quality, although this claim may not be based in fact and should be investigated.

Defendants in these cases may claim at the time of criminal litigation that because the goods are purportedly of equivalent quality to the legitimate goods (or better), they should not be held criminally responsible for their actions. These claims should be considered, along with the following issues:

(1) Whether the defendant used a mark (or packaging) that was substantially similar to the legitimate mark (or packaging), and, if so, the basis of that use;

(2) Whether the defendant compensated the mark holder for (or notified the mark holder of) the defendant's use of its mark;

(3) Whether the defendant marked the goods to indicate to downstream consumers that the goods were not in fact subject to the actual oversight and supervision and would not properly be subject to customer support or warranty coverage as that provided by the mark holder;

(4) Whether the defendant invited any third party to investigate whether the quality control procedures, if any, used were equivalent to those used by the mark holder; and

(5) Whether the defendant provided for equivalent customer support or warranty coverage as that provided by the mark holder, and how downstream consumers were notified of any such support.

A defendant's claims that comparable goods are exempted from the statute would be well-founded for cases of overrun and "grey market" goods. Overrun goods are goods "of which the manufacturer or producer was, at the time of the manufacture . . . in question authorized to use the mark . . . for the type of goods . . . so manufactured . . . by the holder of the right to use such mark or designation." 18 U.S.C. § 2320(e)(1). Thus, if the defendant can show that the OEM was authorized at the time of manufacture to use the mark for the type of good at issue, then his trafficking in goods marked by the OEM may be excluded from criminal liability. Similarly, the defendant may not be criminally liable for selling "gray market goods" – trademarked goods legitimately manufactured and sold oversees and then imported into the United States outside of the trademark owner's distribution channels. See supra Section II.C at page 24.

On the other hand, if the goods do not fall into these exceptions, it may be appropriate to charge trademark counterfeiting. The defendant's claim at trial that the goods are comparable to (or even equivalent to) the legitimate goods would probably not be relevant unless he had identified himself, and not the mark holder, as the true source of and the quality control agent of the marked goods. By using the counterfeit mark without authorization and without any reference to his own role as the actual judge of quality, the defendant has falsely identified the good as authorized by the mark holder and has reaped the profits that are properly due to the mark holder. See United States v. Petrosian, 126 F.3d 1232, 1234 (9th Cir. 1997) ("When 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."), cert. denied, 522 U.S. 1138 (1998). Moreover, if it can be shown that individual consumers are defrauded or deceived by the sale of counterfeit goods, a prosecutor may also charge wire fraud or mail fraud. 18 U.S.C. §§ 1341, 1343. See infra Section VI.B.1 at page 73 (discussing charging wire and mail fraud in infringement cases). The issues of charging a comparable goods case will be exemplified below by a case study of remarked computer chips.

2. A case of comparable goods: Remarked computer chips

Remarked computer chips are representative comparable goods. Because remarking of computer chips can be done in high volume and can provide high margins, they provide an attractive source of revenue. This section will provide market and technical background on computer chip remarking, and then provide a legal analysis of viability of a trademark counterfeiting charge. Such charges have been filed in some districts. 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 <http://www.cybercrime.gov/platinum.htm>. While the legal analysis provided here focuses on remarked computer chips, the legal analysis may also be helpful for other comparable goods cases.

a. Market and technical background on computer chip remarking

It is widely recognized that a computer chip can be operated at a higher standard (e.g., higher speed) than that for which the manufacturer has rated it, just as an extension cord can carry more current than the level at which it has been rated, or an elevator can carry more weight than the amount for which it has been authorized. Manufacturers often deliberately rate their products at a lower operating level to ensure quality control. Some individuals have recognized this practice and taken advantage of it by using the computer chips, or by selling them for use, at the higher speed. Usually, the marks on the chips indicating the manufacturer's suggested speed are removed; and the chips are remarked as capable of performing at the higher speed.

Prosecutors and investigators reviewing remarking cases are faced with the question of whether these practices constitute trademark counterfeiting. This question seems difficult because the original manufacturer's trademark may not have been modified. It is possible that the changes to the chip are to the speed designation and to the wiring without change to the mark.

Chip remarking most commonly takes place with regard to the computer chips known as central processing units ("CPUs"). Intel Corporation is the leading manufacturer of CPUs for use in personal computers, including the "Pentium" line of chips. A CPU is the "brain" of the computer; it is the part of the computer that performs the calculations and operates on the data that is fed into the computer. A chip's speed is measured in "megahertz" or "MHz." For example, a 400 MHz chip is faster than a 300 MHz chip. The speed of the chip, the manufacturer's trademark, and other identifying information are typically etched into the casing of each computer chip.

Faster CPUs command significantly higher prices in the market place than slower CPUs. For example, in May 2000, a legitimate Intel Pentium III 550 MHz CPU could be purchased through legitimate channels for $326, a 650 MHz CPU for $507, and a 733 MHz CPU for $708. Thus, a person could net a 55% profit by remarking a 550 MHz CPU to 650 MHz, or a 40% profit by remarking a 650 MHz CPU to 733 MHz, as long as the chips will perform at the increased speed.

Running a CPU faster than its rated speed can undermine its reliability. A CPU pushed beyond its rating may appear to function properly in many circumstances, but nevertheless fail at some point where a CPU within its rating would not. Typically, the remarking also involves physically altering or hot-wiring the chip so that it will actually function at the faster speed. The process of modifying the CPU may also damage it, either through physical modification of the device or through electro-static discharges into the CPU. Legitimate CPU manufacturers usually take significant quality control steps to safeguard their products from such damage.

b. Charging trademark counterfeiting for trafficking in remarked computer chips

A prosecutor may consider charging trademark counterfeiting for trafficking in remarked computer chips (either manufacturing or reselling them). In response, a defendant may claim that these sales of comparable goods do not constitute trademark counterfeiting, particularly for chips where the speed was remarked, and the trademark itself was unmodified. The defendant may argue that the trademark on the chip was authorized by the mark holder prior to the remarking. Under the case law discussed below, the argument is likely to fail because the use of the trademark in connection with a remarked chip would be considered "counterfeit" within the terms of the statute if there was a lack of quality control by the mark holder when the modifications were made to the chips. (As noted above, if it can be shown that individual consumers are defrauded or deceived by the sale of counterfeit goods, a prosecutor may also charge wire fraud or mail fraud. 18 U.S.C. §§ 1341, 1343. See infra Section VI.B.1 at page 73

(discussing charging wire and mail fraud in infringement cases).)

Few criminal cases have addressed how to determine when a mark placed under circumstances authorized by the mark holder can become a "counterfeit mark." The question is likely to turn on whether the mark can be characterized as a "spurious mark," one that is "not genuine or authentic." 18 U.S.C. § 2320(e)(1)(A); 130 Cong. Rec. 31,675 (1984).

A recent Ninth Circuit case mentioned previously, United States v. Petrosian, 126 F.3d 1232 (9th Cir. 1997), cert. denied, 522 U.S. 1138 (1998), provides the most guidance thus far on the scope of "spurious" in a criminal case. The defendant purchased "genuine Coca-Cola bottles," filled them with a cola-like carbonated beverage that was not Coca-Cola, and told purchasers that the beverage was Coca-Cola. On appeal, the defendant objected to a jury instruction that "counterfeit mark" could include a genuine trademark affixed to packaging containing products not made by, but sold as products of the owner of the registered trademark.

The Ninth Circuit rejected the defendant's contention that the use of the Coca-Cola mark could not be counterfeit because it was a "genuine" mark. Instead, the court defined a spurious mark as "one that is false or inauthentic." Id. at 1234. The court noted 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. The Ninth Circuit's functional analysis thus revolved around the way the mark "falsely indicated" or "falsely identified" the source of a product, without articulating a specific definition for "spurious." Similarly, by selling remarked computer chips with the registered trademark intact, defendants falsely indicate that the remarked chips will perform in accord with manufacturers' quality control standards for chips at that speed.

In interpreting the scope of "counterfeit mark" for purposes of criminal liability, it may be helpful to consider case law under the civil provisions of the Lanham Act. See Section II.B at page 17 (discussing applicability of Lanham Act case law to interpretation of trademark counterfeiting statute). One civil case deserves special attention. In Intel Corp. v. Terabyte Int'l, Inc., 6 F.3d 614 (9th Cir. 1993), the Ninth Circuit affirmed the district court's holding that a distributor of remarked chips was liable under the Lanham Act for trademark infringement. The remarking process involved opening the packages and physically removing or covering the model number that was etched on the chip. Id. at 616. The defendants were distributors of chips remarked by another party. Id. The court rejected the defendant's argument that "confusion as to capability" is irrelevant when there is no confusion as to the source of the product, and recognized that the Lanham Act also protects the right to control the quality of one's goods. Id. at 619. Moreover, the court noted that the remarking activity might be "so basic that it would be a misnomer to call the article by its original name." Id. (citation omitted). Instead of comparing the remarked chips to the original ones (where the defendant could argue that only the label is different), the Ninth Circuit found that "the modified math coprocessors were counterfeit copies of the faster and more expensive models." Id. at 620. Therefore, the defendant's "conduct was

blatant trademark infringement and was prohibited by the Lanham Act." Id. at 623.

In its decision, the Ninth Circuit cites a "quality control" theory and focuses primarily upon the extent of consumer confusion. According to the court, the remarker introduced a defect and took steps so that the customer would not discover the inferior nature of the product. "Intel marked the chip with its name in connection only with the less demanding speed of six megahertz. When the chip genuinely from Intel was marked with a speed designation Intel would not have given it, the chip became a counterfeit . . . ." Id. at 620.

Many courts have recognized that a trademark holder is entitled to maintain at least some degree of control over the continued quality of its trademarked goods, and have been willing to hold defendants liable when the trademarked product is re-manufactured or re-packaged, even though the product might otherwise be considered "genuine." See Champion Spark Plug Co. v. Sanders, 331 U.S. 125 (1947) (affirming injunction against the re-manufacturer of trademarked spark plugs, unless he made sufficient disclosure concerning the re-manufacture to allay customer confusion as to the nature of the mark owner's authorization); Westinghouse Electric Corp. v. General Circuit Breaker & Elec. Supply, Inc., 106 F.3d 894, 899 (9th Cir.) (upholding finding of trademark liability where defendant used Westinghouse mark in connection with reconditioned Westinghouse circuit breakers), cert. denied, 522 U.S. 857 (1997); Shell Oil Co. v. Commercial Petroleum, Inc., 928 F.2d 104, 107 (4th Cir. 1991) (affirming district court's finding that oil was not "genuine" without Shell's enforcement of its own quality controls); El Greco Leather Products Co. v. Shoe World, Inc., 806 F.2d 392, 395-96 (2d Cir. 1986) (holding that the sale of plaintiff's trademarked shoes without the requisite inspection was actionable, since the inspection was a form of quality control and the right to control quality is "[o]ne of the most valuable and important protections afforded by the Lanham Act"), cert. denied, 484 U.S. 817 (1987). See generally Justin D. Swindells, Repackaging Original Trademarked Goods: Trademark Exhaustion or Consumer Confusion?, 7 Fed. Circuit B.J. 391 (1997) (arguing that repackaged, unaltered products can deceive consumers and inflict non-trivial harm on the producer's goodwill). Meaningful disclosure may mitigate trademark liability and defendants may rely upon disclaimers to negate their own culpability, although disclaimers can also be used by prosecutors to show a defendant's awareness of the law and willful violation of it. See infra Section III.E.3 at page 59 (discussing disclaimers).

Although the majority of circuits have found trademark infringement when there is a loss of quality control, "'quality control' is not a talisman the mere utterance of which entitles the trademark owner to judgment." Iberia Food Corp. v. Romeo, 150 F.3d 298, 304 (3d Cir. 1998) (reversing finding of trademark infringement because goods were genuine despite absence of mark holder's quality controls). For example, in some circuits, the court focuses its analysis on the degree of quality control a particular mark owner can expect. This analysis focuses primarily on the mark holder's efforts in maintaining quality control. Id. ("[T]he test is whether the quality control procedures established by the trademark owner are likely to result in differences between the products such that consumer confusion regarding the sponsorship of the products could injure the trademark owner's goodwill."). See also Warner-Lambert Co. v. Northside Dev. Corp., 86

F.3d 3, 6-7 (2d Cir. 1996) (holding that, in order to prove that defendant infringed on plaintiff's trademark by selling trademarked cough drops past their "freshness date," plaintiff must first show that it had a quality control system in place that was not followed by defendant).

The government usually will be able to demonstrate that the trademark holder has extensive quality control procedures related to the speed markings on its chips. The government will often be able to argue it was those quality control procedures that, inter alia, caused the chips to be marked at a lower speed in the first place. Because the quality control procedures that the end user expects are not followed when chips are remarked without the permission of the mark holder, the government should be able to show that trafficking in remarked chips is wrongful conduct as well as a counterfeiting crime.

III. CRIMINAL COPYRIGHT INFRINGEMENT: 17 U.S.C. § 506 & 18 U.S.C. § 2319

Willful copyright infringement is criminalized by 17 U.S.C. § 506(a) in concert with 18 U.S.C. § 2319 for economically motivated infringement or large-scale infringement (even if not committed for commercial gain). Felony penalties attach to violations involving reproduction or distribution of at least ten copies valued at more than $2,500. See 18 U.S.C. § 2319(b)(1). This chapter provides a primer on 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 related to the Internet. Forms providing sample indictments and jury instructions for criminal copyright infringement are provided in Appendix C at page 169. Prosecutors may find other resources to be helpful as well, including treatises, e.g., Melville B. Nimmer & David Nimmer, Nimmer on Copyright Ch. 15 (perm. ed. rev. vol. 1999) (criminal actions), or law review articles. See, e.g., Michael Coblenz, Intellectual Property Crimes, 9 Alb. L.J. Sci. & Tech. 235 (1999); Randy Gidseg et al., Intellectual Property Crimes, 36 Am. Crm. L. Rev. 835 (1999).

In applying these provisions to particular cases, it is helpful to look not only to criminal precedent but also civil precedent. Indeed, courts have noted the "general principle in copyright law of looking to civil authority for guidance in criminal cases." United States v. Wise, 550 F.2d 1180, 1188 n.14 (9th Cir. 1977) (affirming in part and reversing in part conviction for unauthorized sale of copyrighted motion pictures), cert. denied, 434 U.S. 929 (1977), and rehearing denied, 434 U.S. 977 (1977). See also, e.g., United States v. Manzer, 69 F.3d 222, 227 (8th Cir. 1995) (applying the "willfulness" standard used in civil suits); United States v. Cross, 816 F.2d 297, 303 (7th Cir. 1987) (inclusion of civil definitions of copyright infringement in jury instruction on criminal copyright infringement was proper because it is necessary to resort to the civil law of copyright in order to understand the meaning of criminal copyright infringement); Kelly v. L.L. Cool J., 145 F.R.D. 32, 39 (S.D.N.Y. 1992) (conduct that does not support a civil action for infringement cannot constitute criminal conduct), aff'd, 23 F.3d 398 (2d Cir. 1994), cert. denied, 513 U.S. 950 (1994). Prosecutors should be cautioned not to rely unduly upon civil precedent, particularly in areas of sharp differences in the law between civil copyright infringement and criminal copyright infringement; for example, civil infringement can be found with strict liability, whereas a criminal infringement conviction requires a showing of a "willful" intent by the defendant.

A. A Primer on Copyright Law

Copyright law is a complex area of law based on simple principles. A short overview is provided here for those with a passing need to become familiar with this area of law. The central precept of copyright law is:

For a limited time, an original work in fixed form may not be copied (or otherwise infringed) without permission.

Copyright law is intended to protect the creators of original expressive works. Copyright law protects the original expression of an idea or concept in tangible form (be it a novel, a song, a carpet design, or computer source code), but does not extend to protection of the idea or concept itself. Thus, copyright law protects interests distinct from those protected by the patent laws, which provide exclusive rights to inventors of new methods or processes, and the trademark laws, which protect the exclusive use of certain names and slogans in connection with certain goods or services.

A rich body of law has developed to give greater content to this edict, supported by an administrative scheme established and refined by Congress. For federal prosecutors, however, the critical aspects of copyright law can be distilled to a few basic questions: What is the legal basis for creating a "property right" in original intellectual property, such as a book, a movie, or computer software? What are the major developments in federal copyright protection? How does intellectual property become protected by copyright law? Does it need to be registered? How long does that protection last? What counts as "infringement" of a copy? Is infringement really a crime, and, if so, why? What if the infringer was not making any money? These questions will be answered in brief below. A more detailed summary of copyright law is available from many sources and treatises. See, e.g., Melville B. Nimmer & David Nimmer, Nimmer on Copyright (perm. ed. rev. vol. 1999).

What is the legal basis for creating a "property right" in original intellectual property, such as a book, a movie, or computer software? Since 1790, Congress has enacted numerous statutes developing and fine-tuning the copyright law, which is now codified primarily in Title 17 of the United States Code. The Constitution grants Congress both general authority to regulate interstate commerce, U.S. Const. art. I, § 8, cl. 3, and specific authority "[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. "As the text of the Constitution makes plain, it is Congress that has been assigned the task of defining the scope of the limited monopoly that should be granted to authors. . .in order to give the public appropriate access to their work product." Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984) (holding that sale of VCRs does not constitute contributory infringement of television program copyrights because VCRs are capable of substantial non-infringing uses). Thus, "the protection given to copyrights is wholly statutory," id. at 431 (citation omitted), and the remedies for copyright infringement remain confined to "only those prescribed by Congress." Thompson v. Hubbard, 131 U.S. 123, 151 (1889) (citations omitted) (holding that, pursuant to statute, copyright infringements are not actionable unless notice of copyright is provided with both date and name of the person taking it out).

What are the major developments in federal copyright protection? Since 1790, Congress has enacted and repeatedly amended copyright laws, with a trend of continually increased coverage and increased remedies. Beginning in 1909, Congress also imposed criminal penalties for certain types of copyright infringement. See Act of March 4, 1909, ch. 28, 35 Stat. 1082. See, e.g., United States v. Backer, 134 F.2d 533 (2d Cir. 1943) (affirming conviction for

willful infringement for profit of copyrighted figurines).

The major revision in 1976 was a watershed moment in copyright law; it revolutionized copyright law by establishing federal pre-emption over state law. See 17 U.S.C. § 301. Other significant recent legislative developments include: (1) the Computer Software Copyright Act of 1980, Pub. L. No. 96-517, § 10, 94 Stat. 3015 (1980) (codified at 17 U.S.C. §§ 101, 117), which clarified that computer software is entitled to copyright protection; (2) expansion of criminal penalties for certain works in 1982 and for all works in 1992; see 17 U.S.C. § 506 and 18 U.S.C. § 2319; (3) the creation of an exclusive right pertaining to digital audio transmission of sound recordings by the Digital Performance Right in Sound Recordings Act of 1995, Pub. L. No. 104-39, 109 Stat. 336 (1995); (4) the criminalization of large-scale copying even in the absence of economic motivation by the No Electronic Theft (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997); (5) the 1998 extension of the term of copyrights; see Sonny Bono Copyright Term Extension Act, Pub. L. No. 105-298, 112 Stat. 2827 (1998); and (6) the Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified at 17 U.S.C. §§ 1201-1205).

How does intellectual property become protected by copyright law? Does it need to have been registered with the Copyright Office? Congress has provided copyright protection to 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). This definition has two components, originality and fixation, which set the outer limits of federal copyright protection. While copyright protection exists from the time of the creation of a work, see 17 U.S.C. §§ 101-102(a), civil infringement actions may be brought only with respect to those works that have been registered with the Register of Copyrights. 17 U.S.C. §§ 411, 412. Similarly, criminal prosecutions should be sought only after the infringed works have been registered.

How long does copyright protection last? The term of copyright protection for works created in 1978 or later is life of the author plus seventy years. See 17 U.S.C. § 302(a). Pre-1978 works are protected for ninety-five years from the date of creation. See 17 U.S.C. § 304. Corporate copyrights are treated similarly. See 17 U.S.C. § 304.

What constitutes "infringement" of a copyrighted work? Generally, infringement is the violation of one of five exclusive rights granted to a copyright owner by federal law. The five exclusive rights are: (1) reproduction, (2) distribution, (3) public display, or (4) public performance of the copyrighted work, as well as (5) preparation of derivative works based upon the original copyrighted work. See 17 U.S.C. § 106(1)-(5). "An unlicensed use of the copyright is not an infringement unless it conflicts with one of the[se] specific exclusive rights conferred by the copyright statute." Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 447 (1984) (citation omitted) (holding that sale of VCRs does not constitute contributory infringement of television program copyrights because VCRs are capable of substantial non-infringing uses). In

addition to these five exclusive rights applicable to all copyrighted works, the Digital Performance Right in Sound Recordings Act of 1995, Pub. L. No. 104-39, 109 Stat. 336 (1995), codified at 17 U.S.C. § 106(6), established a sixth exclusive right pertaining to digital audio transmission of sound recordings. See also 17 U.S.C. § 101 (defining "sound recording" to exclude audiovisual works); 17 U.S.C. § 114(j)(3) (excluding transmission of audiovisual works from the definition of "digital audio transmission"); 17 U.S.C. § 114(d)-(j) (limitations including exemptions for certain broadcast transmissions, subscription transmissions, and licensed transmissions).

What makes copyright infringement a crime? Is it a felony? Copyright infringement is a crime where it is done willfully and either: (1) for commercial advantage or private financial gain, 17 U.S.C. § 506(a)(1); or (2) by reproduction or distribution on a large scale (i.e., copying works with a total retail value of over $1,000), 17 U.S.C. § 506(a)(2). Felony punishment is provided only for reproduction or distribution of at least 10 copies during any 180 days of copyrighted works worth more than $2,500. 18 U.S.C. § 2319(b)-(c). The reason that copyright infringement is a crime is to punish and deter the misappropriation of intellectual property that an author — who may have no means to prevent copying — invested time, energy and money to create.

Is copyright infringement a crime under 17 U.S.C. § 506(a) and 18 U.S.C. § 2319 if the infringer is not making any money? Yes, if the infringement is reproduction or distribution done willfully on a large scale. Although punishment can be more harsh if the infringer has pecuniary motives, willful infringement by reproduction or distribution of at least 10 copies during any 180 days of copyrighted works worth more than $2,500 is a felony, punishable by up to three years in prison and a fine, even if not done for commercial gain. See 18 U.S.C. § 2319(c). Even if the infringer is not profiting from his or her actions, he or she is facilitating the theft of intellectual property from its creator. Because intellectual property can be disseminated so cheaply in digital format over computer media (like the Internet), the criminal law can play an important role protecting the rights of copyright owners.

What other criminal laws protect copyrighted material besides 17 U.S.C. § 506(a) and 18 U.S.C. § 2319? A number of other federal laws specifically protect copyrighted works. 18 U.S.C. § 2318 prohibits the counterfeit labeling of copyrighted works. Further, in 1994, Congress created 18 U.S.C. § 2319A, which expressly covers the unauthorized "fixation" of and trafficking in recordings and musical videos of live musical performances. Pub. L. No. 103-465, Title V, § 513(a), 108 Stat. 4974 (1994). Systems of copyright management are protected by 17 U.S.C. § 1201 and § 1202. 17 U.S.C. § 506 also provides lesser criminal sanctions for conduct which does not constitute copyright infringement but which nonetheless undermines the integrity of the copyright system, such as for false representations in copyright applications. See 17 U.S.C. § 506(c)-(e).

A significant number of other federal statutes are important in copyright cases. For example, most large-scale copyright cases involve the unauthorized use of a trademark in

violation of 18 U.S.C. § 2320; for instance, infringing copies of movies will typically be sold with packaging bearing the trademark of the rightful owner of distributor. In addition, other criminal laws, from the familiar such as mail and wire fraud, 18 U.S.C. §§ 1341, 1343, to the obscure, such as unauthorized reception of cable service, 47 U.S.C. § 553, or the unauthorized use of communications, 47 U.S.C. § 605, can be applicable as well.

B. The Elements of Copyright Infringement (Felony and Misdemeanor)

There are four essential elements to a charge of felony copyright infringement. In order to obtain a felony conviction under 17 U.S.C. § 506(a) and 18 U.S.C. § 2319, the government must demonstrate that:

(1) A copyright exists, see infra Section III.B.1 at page 39;

(2) It was infringed by the defendant by reproduction or distribution of the copyrighted work, see infra Section III.B.2 at page 40;

(3) The defendant acted willfully, see infra Section III.B.3 at page 43; and

(4) 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. See infra Section III.B.4 at page 46.

See 17 U.S.C. § 506(a)(2); 18 U.S.C. § 2319(a), (c)(1). The maximum punishment for this crime is 3 years imprisonment and $250,000. See infra Section III.D at page 55.

Another element, if proven, enhances the maximum penalty: That the defendant acted "for purposes of commercial advantage or private financial gain." If it is proven, the statutory maximum prison sentence can rise to 5 years. See 17 U.S.C. § 506(a)(1); 18 U.S.C. § 2319(a), (b)(1). See also infra Section III.B.5 at page 47 (discussing commercial purposes element). Moreover, a commercial motivation case will usually have better jury appeal than a case without commercial motivation. Indeed, if commercial motivation is not alleged, defendants may be more inclined to raise the affirmative defense of fair use, codified at 17 U.S.C. § 107, since fair use defenses are more plausible when defendants do not profit financially by their acts of infringement. For a discussion of "fair use," see infra Section III.C.3 at page 53.

Misdemeanor copyright infringement is another option for prosecutors. It can be a useful charge in cases where scale of the crime is difficult to prove with specificity, such as a video store engaging in copying of video tapes without records showing when those copies were made, or how many of those copies were made. See infra Section III.B.6 at page 49.

Prosecutors should also be aware of an important defense that is sometimes treated as an element of the crime. A minority of courts also require that the government prove the absence of

a "first sale." Some cases refer to this as a "fifth element." See infra Section III.C.2 at page 50.

The statutes governing criminal copyright infringement were substantially amended in 1997. No Electronic Theft Act (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997). These amendments modified the requisite elements for the crime. Notably, the proof of commercial or financial motivation is no longer required for a felony conviction. Consequently, criminal copyright infringement cases pre-dating the NET Act are of limited utility for setting out the elements of the crime. See, e.g., United States v. Manzer, 69 F.3d 222, 227 (8th Cir. 1995) (infringement of computer program used in satellite descrambler modules); United States v. Hux, 940 F.2d 314, 319 (8th Cir. 1991) (affirming, in relevant part, copyright infringement conviction for manufacture of modified satellite descrambler devices), overruled on other grounds by United States v. Davis, 978 F.2d 415 (8th Cir. 1992); United States v. Wise, 550 F.2d 1180 (9th Cir.) (affirming in part and reversing in part conviction for unauthorized sale of copyrighted motion pictures), cert. denied 434 U.S. 929 (1977), and rehearing denied, 434 U.S. 977 (1977). Nevertheless, since the substance of many of the specific elements were unchanged, the cases pre-dating the NET Act are of use in interpreting the current elements.

1. Existence of a copyright

The initial element of a criminal prosecution under 17 U.S.C. § 506(a) is that the victim has a copyright. The copyright is typically established by production of a certificate of registration from the Register of Copyrights. While copyright protection exists from the time of the creation of a work, see 17 U.S.C. §§ 101-102(a), infringement actions may be brought only with respect to those works that have been registered with the Register of Copyrights. 17 U.S.C. §§ 411, 412. Since this requirement is recognized as a mere formality, "once such a registration has occurred, a subsequent infringement action could be for infringing acts that occurred either after, or prior to the registration." Melville B. Nimmer & David Nimmer, Nimmer on Copyright § 7.16[B][1][a], at 7-153 (perm. ed. rev. vol. 1999) (citing Pittway Corp. v. Reliable Alarms Mfg. Corp., 164 U.S.P.Q. 379, 380 (E.D.N.Y. 1969) ("Delay in obtaining the copyright certificate does not affect the validity of a copyright, so long as the work has been published with a proper copyright notice.")[5] and Primcot Fabrics v. Kleinfab Corp., 368 F. Supp. 482, 484 (S.D.N.Y. 1974) (rejecting contention that "failure to register the copyright until after the defendant began his own publication" is fatal)). Accord Washingtonian Pub. Co. v. Pearson, 306 U.S. 30, 39 (1939) ("Petitioner's claim of copyright came to fruition immediately upon publication. Without further notice it was good against all the world. Its value depended upon the possibility of enforcement. The use of the word 'until' in section twelve [now Section 411] rather than 'unless' indicates that mere delay in making deposit of copies was not enough to cause forfeiture of the right theretofore distinctly granted.").

---

[5] Since March 1, 1989, copyright "notice is no longer required at publication, and absence of notice will no longer consign a work to the public domain." Melville B. Nimmer & David Nimmer, Nimmer on Copyright § 7.02[C][3], at 7-17 (perm. ed. rev. vol. 1999).

Criminal prosecutions should be sought only after the infringed works have been registered, although technical irregularities in the registration process will not invalidate an otherwise proper registration. United States v. Backer, 134 F.2d 533, 535-36 (2d Cir. 1943). But compare United States v. Gallo, 599 F. Supp. 241, 245 n.1 (W.D.N.Y. 1984) ("Of course, there can be no infringement or illegal distribution until a game [work] is protected by a copyright. In the case of PENGO [one of the works at issue,] the government must prove enough instances of distribution occurring after its November 2, 1982, registration date to fulfill the statutory requirements. Evidence 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.") with Melville B. Nimmer & David Nimmer, Nimmer on Copyright § 15.01[A][2], at 15-4 & n. 24 (perm. ed. rev. vol. 1999) (characterizing Gallo as "erroneously assuming that registration is a condition precedent to obtaining copyright rather than to bringing an infringement action").

By law, a certificate of registration "made before or within five years after the first publication of the work shall constitute prima facie evidence of the validity of the copyright." 17 U.S.C. § 410(c). See also United States v. Taxe, 540 F.2d 961, 966 (9th Cir.) (certificate of registration provided prima facie proof of date of fixation), cert. denied, 429 U.S. 1040 (1976). Where a copyright registration certificate is produced, the burden shifts to the defendant to present evidence that the copyright is not genuine, not valid, or fraudulently obtained. See, e.g., Autoskill, Inc. v. National Educ. Support Sys., Inc., 994 F.2d 1476, 1487 (10th Cir. 1993) (affirming grant of preliminary injunction for infringement of copyright in software and finding that "[b]y introducing the registration certificate in which it identified itself as the author, then, Autoskill presented prima facie evidence that it was the owner of the copyright"). If the defendant contests the copyright, the prosecutor may present evidence showing that a copyright is genuine, properly obtained, and valid.

If more than five years elapse between the first publication of a work and its registration, the court has discretion to determine the evidentiary weight given to the registration certificate in deciding validity of copyright. See, e.g., Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 923 F. Supp. 1231, 1241 (N.D. Cal. 1995) ("When registration is made more than five years after first publication, the evidentiary weight of the certificate of registration is within the court's discretion."); Koontz v. Jaffarian, 617 F. Supp. 1108, 1111-12 (E.D. Va. 1985) (original manual registration is prima facie evidence of valid copyright, but because revised versions of same manual were not registered within five years, court has discretion to decide evidentiary weight of registration for revised versions), aff'd 787 F.2d 906 (4th Cir. 1986).

2. Infringement of the copyright (by reproduction or distribution of the copyrighted work)

Once the copyright is established, the government must then prove that the defendant "infringed" that copyright. See 17 U.S.C. § 506(a). Although the term "infringement" is not

defined per se in the copyright statute, 17 U.S.C. § 501(a) provides that: "[a]nyone who violates any of the exclusive rights of the copyright owner as provided by [17 U.S.C. §§ 106-121] . . . is an infringer of the copyright." Thus, the concept of infringement can be defined by reference to the exclusive rights conferred on a copyright owner by 17 U.S.C. § 106. Those exclusive rights include, most importantly, the right to reproduce and distribute copies of the work, 17 U.S.C. § 106(1)-(3), along with the right to prepare derivative works, 17 U.S.C. § 106(2), or to display or perform the work publicly, 17 U.S.C. § 106(4)-(6).

Felony copyright infringement is applicable only where the defendant violates the two most important rights of reproduction and distribution. See 18 U.S.C. § 2319(b)(1) (providing a felony penalty only when the offenses consists of "reproduction or distribution"); see also 18 U.S.C. § 2319(c)(1) (same). In cases alleging felony violations, proof of infringement typically involves evidence that the defendant copied one or more copyrighted works or sold unauthorized copies of one or more works. There is no requirement that the defendant have "stolen" the original work. Infringement may be found when the defendant bought a legal copy from which he or she has made the illegal copies.

Traditional copyright infringement by reproduction is done by making direct copies onto physical media – one at a time. For example, a person may hook together video-cassette recorders and copy a videotape from one VCR to others. More sophisticated infringers might duplicate CD-ROMs with complex machines. These classic means of direct reproductions without authorization represent the clearest cases of copyright infringement. The Internet facilitates infringement — particularly reproduction and distribution — in a variety of novel ways. See generally Section III.E at page 56 (discussing Internet-based copyright infringement).

Statutory exceptions. A few statutory exceptions deserve brief note. For example, under 17 U.S.C. § 109(b)(4), the unauthorized rental, lease, or lending of a phonorecord or software, while subject to civil sanctions, is not a criminal offense under 17 U.S.C. § 506. Moreover, for computer software, 17 U.S.C. § 117 specifically permits software copying under two narrow exceptions - the "archival" exception and the "essential step" exception. The "archival" exception permits a lawful owner to make one backup software copy against the risk of destruction of the original by disk failure, system crash, or other mechanical or electrical failure. See 17 U.S.C. § 117(a)(2). The "essential step" exception permits a person who lawfully owns one copy of the software to load the program into a computer for use, thus creating a second copy, without infringing the copyright. See 17 U.S.C. § 117(a)(1); see, e.g., Micro-Sparc, Inc., v. Amtype Corp. , 592 F. Supp. 33 (D. Mass. 1984) (purchasers of programs sold in printed form do not infringe copyright by typing code into computer in order to use the programs); Summit Techs., Inc. v. High-Line Med. Instruments Co., 922 F. Supp. 299 (C.D. Cal. 1996) (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) (loading of copyrighted software into RAM by service company constitutes reproduction), cert. dismissed, 510 U.S. 1033 (1994).

Proof of Infringement. Infringement by reproduction can be clearly established by direct evidence of copying. However, since the actual infringement of the copyrighted work is not often provable in reproduction cases, circumstantial evidence may be used to prove that (1) the defendant had access to the copyrighted work and (2) that defendant's work is substantially similar to the copyrighted material. Kepner-Tregoe, Inc. v. Leadership Software, Inc., 12 F.3d 527, 532 (5th Cir.) ("As direct evidence of copying is uncommon, plaintiffs generally demonstrate copyright infringement indirectly or inferentially by proving that (1) defendants had access to the copyrighted works, and (2) there is a substantial similarity between infringed and infringing works."), cert. denied, 513 U.S. 820 (1994); see also Computer Associates Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 701 (2d Cir. 1992) (affirming holding that compatibility components of computer programs were not substantially similar) (subsequent history omitted); Kamar Int'l, Inc. v. Russ Berrie & Co., 657 F.2d 1059, 1062 (9th Cir. 1981) (discussing similarity standard with regard to copyright of design of stuffed animals). If the copyrighted work and the defendant's work are strikingly similar, the first element of access may be assumed without proof, especially when the copyrighted work is widely available. See, e.g., Playboy Enters. v. Frena, 839 F. Supp. 1552, 1556 (M.D. Fla. 1993) (proof of access not necessary when defendant made "essentially exact" copies of copyrighted photos which appeared in nationally circulated magazine).

It is unnecessary to demonstrate that an allegedly infringing article is identical to the original work in all respects. See United States v. O'Reilly, 794 F.2d 613, 615 (11th Cir. 1986) (affirming conviction for infringement of copyright in video games). Instead, infringement may be shown by simply demonstrating a "substantial similarity" between the original work and the suspect copy. See, e.g., McCulloch v. Albert E. Price, Inc., 823 F.2d 316, 318-19 (9th Cir. 1987) (holding that all elements, including noncopyrightable elements, should be considered as a whole in assessing infringement of a copyrighted plate). A copy has been held to be "substantially similar" to an original work where "the [copy] is so similar to the [original] work that an ordinary reasonable person would conclude that the defendant unlawfully appropriated the [copyright owner's] protectible expression by taking material of substance and value." Atari, Inc. v. North American Philips Consumer Elec. Corp., 672 F.2d 607, 614 (7th Cir.) (citation omitted) (reversing denial of preliminary injunction for infringement of copyright in video game), cert. denied, 459 U.S. 880 (1982). This standard focuses on the similarities between the two works, rather than on differences that may exist between them. 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." O'Reilly, 794 F.2d at 615 (quoting Sheldon v. Metro-Goldwyn Pictures Corp., 81 F.2d 49, 56 (2d Cir.) (L. Hand, J.), cert. denied, 298 U.S. 669 (1936)). But infringement requires more than evidence of adherence to the general ideas expressed, because ideas in and of themselves cannot be copyrighted. See 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."); Hoehling v. Universal City Studios, Inc., 618 F.2d 972, 977 (2d Cir.) (affirming summary judgment for defendants on ground that historical interpretation is not copyrightable), cert. denied, 449 U.S. 841 (1980).

In practice, substantial similarity is generally demonstrated through a side-by-side

comparison of the suspect copy with an authentic original. In several instances, defendants have argued that the government must compare these allegedly infringing copies against the originals maintained on file at the Register of Copyrights in order to satisfy its burden of proof on this issue. See O'Reilly, 794 F.2d 613, 615 (11th Cir. 1986); United States v. Shabazz, 724 F.2d 1536, 1539 (11th Cir. 1984) (affirming conviction for criminal infringement of copyright in tape recordings). While some courts have agreed "that it is 'better practice' for the Government to compare the counterfeit material with the duplicate registered with the Copyright Office," O'Reilly, 794 F.2d at 615, no court has accepted this defense argument. Thus, any authentic duplicate of the original may be used for the purpose of making this comparison.

3. The defendant acted "willfully"

To establish criminal intent, the government must prove that the defendant willfully infringed the copyright. See 17 U.S.C. § 506(a). Congress amended 17 U.S.C. § 506(a) in the No Electronic Theft (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997), to state that "evidence 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). The statute was amended to require 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. S12689 (daily ed. Nov. 13, 1997). Despite this helpful clarification, the legislation provides no definition of "willful infringement," reaffirming the Supreme Court's observation 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).

The omission by Congress of an affirmative definition illustrates the sharply differing views held by members of Congress on the meaning of "willful." On the one hand, Senator Hatch, the Chairman of the Senate Judiciary Committee, suggested that "'willful' ought to mean the intent to violate a known legal duty." 143 Cong. Rec. S12689 (1997) (daily ed. Nov. 13, 1997) (citing Cheek v. United States, 498 U.S. 192 (1991)). In the House, on the other hand, Representatives Goodlatte and Coble, who introduced and sponsored the bill, emphasized that:

> 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. H9884, H9886 (daily ed. Nov. 4, 1997).

Courts addressing this issue have not standardized any formulaic definition of the term "willful" as applied to copyright infringement prosecutions. For example, the Seventh Circuit, in United States v. Cross, 816 F.2d 297 (7th Cir. 1987), approved without comment the jury

instruction that a willful act is an act 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." Id. at 300. The Cross court affirmed the infringement conviction because there was ample evidence on the record that the defendant "knowingly and voluntarily violated the copyright laws." Id. at 300-01. In a case decided prior to Cross, the Seventh Circuit likewise concluded on the facts presented that 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,'" the government had met its burden of proving willfulness. United States v. Heilman, 614 F.2d 1133, 1138 (7th Cir.) (quoting trial court), cert. denied, 447 U.S. 922 (1980). In United States v. Moran, 757 F. Supp. 1046, 1049 (D. Neb. 1991), the district court concluded that willful infringement means a "'voluntary intentional violation of a known legal duty'" (quoting Cheek v. United States, 498 U.S. 192, 200 (1991)).[6] One academic has lamented the "uncertainty" of the willfulness standard in criminal copyright infringement cases. 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).

The Tenth Circuit has held that where the government presented "enough" evidence on the issue of willfulness and intent, it had no additional "duty to anticipate the defendants' evidence" where the defendant attempted "to present evidence sufficiently convincing to the jury to blunt the thrust of the government's proof." United States v. Sherman, 576 F.2d 292, 297 (10th Cir.), cert. denied, 439 U.S. 913 (1978). In that case, despite the defendant's claim of good faith reliance on a contract asserting that the supplied tapes were "sound-a-like" simulations of original artists, the circuit court concluded that the jury either disbelieved the genuineness of the contract or believed that the defendants were not innocent of knowledge that the tapes provided were copies from the original artists' records, i.e., the jury may have believed that the defendants knew that the provided tapes were themselves pirated. Id.

Despite the diverse language courts have used to formally define willfulness in the context of copyright infringement, experience teaches that certain types of evidence have been found particularly relevant finding the defendant's intent:

- Evidence that the defendant had legal notice conduct similar to his was infringement. See United States v. Heilman, 614 F.2d 1133, 1138 (7th Cir.) (affirming conviction of defendant aware that Department of Justice was prosecuting individuals engaged in conduct similar to his own and that conduct

---

[6] The Supreme Court in Cheek recognized the general principle that "ignorance of the law or a mistake of law is no defense to criminal prosecution." Cheek, 498 U.S. at 199. However, the Court concluded that given the complexity of the federal criminal tax statutes, a good faith misunderstanding of the legal duties imposed by the tax laws negated a finding of willfulness. This reasoning has been applied in other contexts as well. See, e.g., Ratzlaf v. United States, 510 U.S. 135 (1994) (failure to report cash transactions in excess of $10,000).

had been ruled illegal by four circuit courts and three state courts), cert. denied, 447 U.S. 922 (1980).

- Evidence that the defendant had in the past manufactured and distributed pirated tapes. See United States v. Whetzel, 589 F.2d 707, 712 (D.C. Cir. 1978) (holding prior acts of manufacturing and distributing pirated tapes probative of defendant's state of mind).

- Evidence that defendant had actual notice that his own conduct was illegal. See United States v. Cross, 816 F.2d 297, 300-01 (7th Cir. 1987) (affirming conviction where defendant continued to sell pirated videotapes after FBI agents informed him that sale and rental of unauthorized tapes was illegal).

- Evidence that the defendant acknowledged his or her conduct was improper. See United States v. Manzer, 69 F.3d 222, 227-28 (8th Cir. 1995) (upholding conviction where defendant in a written interview published in newsletter admitted that selling or giving away copyrighted computer chips was illegal and where software program and plastic module containing software bore notice of copyright); United States v. Drebin, 557 F.2d 1316, 1324 (9th Cir. 1977) (affirming conviction where defendant warned customers of FBI investigation and recommended that customers be "really careful"), cert. denied, 436 U.S. 904 (1978); United States v. Hux, 940 F.2d 314, 319 (8th Cir. 1991) (upholding conviction where defendant admitted in FBI interview 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) (affirming that prosecutor properly argued to jury that defendant was guilty of willful infringement by soliciting attorney to lie about legality of tapes), cert. denied, 429 U.S. 1040 (1977).

Other factors may be relevant to finding an absence of "willfulness":

- Evidence that the defendant had a good-faith belief that the 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) (finding police officer not guilty who operated a "mom-and-pop" video rental business and made single copies of lawfully purchased videos and rented the copied tapes only (for purposes of preventing vandalism of original tapes), and whose activities were "conducted in such as way as to not 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.) (affirming conviction where evidence did not support assertion of good-faith belief that tapes manufactured and sold were "sound-alikes" and therefore not protected by the copyright statute), cert. denied, 439 U.S. 913 (1978).

If willfulness is difficult to show on the facts of a particular case, the prosecutor should seriously consider charging another crime, such as 18 U.S.C. § 2318, which prohibits trafficking in counterfeit labels affixed or designed to be affixed to copyrighted works; such labels are present in many copyright cases, and, for intent, prosecutors need prove only that the label trafficking was done "knowingly." See infra Section IV.A at page 67.

4. 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

For the fourth element, 18 U.S.C. § 2319 provides a felony penalty when the infringement 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); see also 18 U.S.C. § 2319(c)(1) (alternative felony provision). Some of these technical requirements may be difficult to prove on the facts of a particular case. For example, if a search reveals that the defendant was operating a video rental store where all the videos were pirated but no business records were kept, it may be difficult to prove that the defendant himself reproduced the pirated videos, or distributed them, or that he did so within a particular 180-day period. If faced with such a case, the government may consider charging misdemeanor copyright infringement, which reduces the number of copies to 1 and the retail value threshold to $1,000. See infra Section III.B.6 at page 49 (discussing misdemeanor copyright infringement). Alternatively, if the pirated video tapes had counterfeit labels, prosecutors could consider charging 18 U.S.C. § 2318, which provides felony punishment for the counterfeit labeling of copyrighted works without requiring proof of any particular minimum number of copies made in a particular time period. See supra Chapter IV at page 66. A third option would be to charge the defendant with violating 18 U.S.C. § 2320, if the pirated videotapes were marked with counterfeit marks. See supra Chapter II at page 15.

A brief discussion follows regarding the meaning of some of these technical requirements: (1) the definition of copies; (2) the reason for minimum of 10 copies; (3) the purpose of "one or more copyrighted work" language; (4) the definition of "retail value" in this context; and (5) the $2,500 minimum. For a discussion of the units of prosecution to charge, see infra Section VI.C at page 101.

Definition of copies. "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. The statute notes specifically that the term "includes the material object, other than a phonorecord, in which the work is first fixed." Id.

Reason for minimum of 10 copies. Requiring a minimum of 10 copies was intended to exclude from felony prosecution "children making copies for friends as well as other incidental

copying of copyrighted works having a relatively low retail value." H.R. Rep. No. 102-997, at 6 (1992), reprinted in 1992 U.S.C.C.A.N. 3569, 3574.

Purpose of "one or more copyrighted work" language. The drafting Committee explained that the reason for the phrase "of one or more copyrighted works" was that it "intended to permit aggregation of different works of authorship to meet the required number of copies and retail value." Id. The Committee gave an example of a defendant's reproduction of 5 copies of a copyrighted word processing computer program having a retail value of $1,300 and the reproduction of 5 copies of a copyrighted spreadsheet computer program also having a retail value of $1,300. The Committee specifically noted that this aggregation "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.

Definition of "retail value" in this context. The drafting Committee 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.

The Committee acknowledged, however, that copyrighted works can be infringed before a retail value has been established – as is the case with software "beta-test" versions. (Beta test copies of software are those still under development that have not yet been sold to the public. They are circulated to selected users for testing and evaluation. At the time they are circulated, however, the copyright holder may not have established the eventual retail price.) The Committee left it to the courts, in such cases, to look to the "suggested retail price, the wholesale price, the replacement cost of the item, or financial injury caused to the copyright owner." Id. at 7; 1992 U.S.C.C.A.N. at 3575. In any case, the term "retail value" in this provision was intended to refer to the retail value of the infringed item, i.e., the genuine item that was infringed.

$2,500 minimum. In order to charge a felony violation of the criminal copyright statute, the government must also prove that the infringing copies have a total retail value of more than $2,500. There is one minor snare on the $2,500 threshold of which prosecutors should be aware: In cases where a profit motive is shown, the trigger for felony penalties is a combined retail value of "more than" $2,500, 18 U.S.C. § 2319(b)(1), whereas without showing a profit motive, the threshold is a combined retail value of "$2,500 or more." 18 U.S.C. § 2319(c)(1). For a felony charge, prosecutors should be careful simply to charge a value greater than $2,500.

5. Enhancing element: Purposes of commercial advantage or private financial gain

Another element can provide an enhancement to the maximum punishment: That the defendant acted "for purposes of commercial advantage or private financial gain." 17 U.S.C. § 506(a)(1). Prior to the 1997 amendments, this element was required to prove any federal copyright crime. Cf. United States v. LaMacchia, 871 F. Supp. 535, 539-40 (D. Mass. 1994) (dismissing wire fraud charges brought against defendant who engaged in large-scale non-

commercial copying by means of the Internet). These amendments reflect Congressional recognition that the Internet provides a growing means for large-scale electronic piracy that has a substantial market impact, even where the infringer does not have a profit motive. See H.R. Rep. No. 105-339, at 4 (1997). Software copying and distribution on the Internet are inexpensive and easy, thus reducing infringers' economic need for a financial return when making and distributing copies. Willful infringers may be driven by a variety of non-profit motives, including a rejection of the copyright laws, anti-corporate sentiments, or a desire to gain respect in the Internet community. These willful large-scale infringers may be driven by a financial motivation that may be difficult to articulate or prove to a jury.

While this element is now not required for a felony conviction, it is often worth considering in charging a case. If it is proven, the statutory maximum prison sentence can rise to 5 years, rather than 3 years. See 17 U.S.C. § 506(a)(1); 18 U.S.C. § 2319(a), (b)(1). This element is also an alternative fourth element under a misdemeanor copyright charge. See infra Section III.B.6 at page 49 (discussing misdemeanor copyright infringement). Moreover, a commercial motivation case will usually have better jury appeal than a case without commercial motivation. Indeed, if commercial motivation is not alleged, defendants may be more inclined to raise the affirmative defense of fair use, codified at 17 U.S.C. § 107, since fair use defenses are more plausible when defendants do not profit financially by their acts of infringement. For a discussion of "fair use," see infra Section III.C.3 at page 53.

Where the government must prove that the defendant willfully infringed "for purposes of commercial advantage or private financial gain," the emphasis should be placed on "purposes," for it is irrelevant whether any profit was in fact realized. See 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, 540 F.2d 961 (9th Cir. 1976), cert. denied, 429 U.S. 1040 (1977). All that is required is that the defendant engage in the infringing conduct with the hope or expectation of profit. In some cases, courts have found the requisite commercial or financial purpose to be implicit in the conduct of the parties. See United States v. Cross, 816 F.2d 297, 301 (7th Cir. 1987) ("[W]e find that the presence of these seventeen second-generation videocassettes on [subject's] business premises may rationally give rise to the inference that they were maintained for commercial advantage or private financial gain."). Accord United States v. Shabazz, 724 F.2d 1536, 1540 (11th Cir. 1984) ("not necessary that [the defendant] actually made a profit") (citing United States v. Wise, 550 F.2d 1180, 1195 (9th Cir.), cert. denied, 434 U.S. 929 (1977)); United States v. Moore, 604 F.2d 1228, 1235 (9th Cir. 1979) ("[I]t is irrelevant whether there was an exchange for value so long as there existed the hope of some pecuniary gain.") (citing Taxe).

Because the statute plainly requires a "purpose" of commercial advantage or financial gain, many different methods of showing a profit motive can be relevant in copyright cases.

Evidence of discrete monetary transactions, whether selling infringing works separately or bundled with computer hardware, provides the best evidence of financial gain. Other evidence could include a showing that the infringers used illicit software "libraries" as a major incentive to attract individuals to a bulletin board or Web site, if the individuals are required to pay a subscription fee or if advertising space is sold. In addition, reproduction of unauthorized copies of a work for use within a single company is clearly an infringement for financial gain and commercial advantage. Although the infringer may not expect to receive money or other items of value for the infringing copies, the purpose of the infringement is to save money by not purchasing additional authorized copies or licenses; the savings constitutes a financial gain for the infringer that allows the infringer to gain a commercial advantage over competitors who use only licensed copies of copyrighted work.

Bartering represents another type of financially motivated transaction within the terms of the statute. In "bartering" schemes, people trade infringing copies of a work for other items, including computer time or infringing copies of other works, as either a one-for-one exchange or through the use of credit or "points" systems. "Financial gain" is defined to include the "receipt, or expectation of receipt, of anything of value, including the receipt of other copyrighted works." 17 U.S.C. § 101 (emphasis added). Under this definition, it is clear that if the infringer receives or expects to receive anything of value, including copies of other works, he or she has infringed for financial gain. This definition was specifically added with the passage of the NET Act to address cases involving bartering. See No Electronic Theft Act (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997). See 143 Cong. Rec. S12689 (1997) (daily ed. Nov. 13, 1997) (statement of Sen. Hatch); 143 Cong. Rec. H9885 (daily ed. Nov. 4, 1997) (statement of Rep. Goodlatte).

6. Misdemeanor copyright infringement

Misdemeanor copyright infringement can be a useful charge in cases where scale of the crime is difficult to prove with specificity, such as a video store engaging in copying of video tapes without records showing how many copies were made or when those copies were made. Misdemeanor copyright infringement, for which the maximum penalty is one year in prison and a fine of $100,000, has almost the same first three elements as felony copyright infringement. One difference is that felony copyright infringement is committed, as noted above, only where the infringement is by reproduction or distribution. See supra Section II.B.2 at page 40 (discussing infringement requirements for felony copyright crime). For the last element, either the government must prove either a smaller scope and quantity of infringement (only one copy with only a retail value of $1,000), see 17 U.S.C. § 506(a)(2); 18 U.S.C. § 2319(a), (c)(3), or, no quantity at all if the government proves that the defendant acted "for purposes of commercial advantage or private financial gain." See 17 U.S.C. § 506(a)(1); 18 U.S.C. § 2319(a), (b)(3).

Thus, while many of the elements for misdemeanor copyright infringement are substantively similar to the elements for felony copyright infringement, the government's burden for proving scope or scale can be somewhat lessened. The substance of the elements themselves can be analyzed by reference to the analogous felony element.

In short, in order 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, see supra Section III.B.1 at page 39;

(2) it was infringed by the defendant, see supra Section III.B.2 at page 40;

(3) the defendant acted willfully, see supra Section III.B.3 at page 43; and

(4) the infringement was done EITHER

(a) for purposes of commercial advantage or private financial gain, see supra Section III.B.5 at page 47; 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, see supra Section III.B.4 at page 46.

C. Defenses to Criminal Copyright Infringement

1. Statute of limitations: 5 years

The criminal copyright statute has a five-year statute of limitations, making it consistent with most other criminal statutes. 17 U.S.C. § 507 now provides that "no criminal proceeding shall be maintained under the provisions of this title unless it is commenced within 5 years after the cause of action arose." Until passage of the NET Act in 1997, copyright violations had been subject to a three-year statute of limitations.

2. The "first sale" doctrine in criminal cases

The "first sale" doctrine limits the copyright owner's "exclusive rights" to authorize or distribute copies of a copyrighted work to the public under 17 U.S.C. § 106(3). It provides that a sale of a "lawfully made" copy terminates the copyright holder's authority to interfere with or control subsequent sales or distributions of that particular copy. See 17 U.S.C. § 109(a). See United States v. Moore, 604 F.2d 1228, 1232 (9th Cir. 1979) ("[W]here a copyright owner parts with title to a particular copy of his copyrighted work, he divests himself of his exclusive right to vend that particular copy."). In short, through the first sale doctrine, the first purchaser and any subsequent purchaser of that specific copy of a copyrighted work receive the right to sell, display or dispose of their copy. If copyright owner A sells a copy of a work to B, B may sell that particular copy without violating the law. B does not, however, receive the right to reproduce and distribute additional copies made from that work. Thus, if B makes any unauthorized copies of that work, he or she violates the law.

Criminal defendants sometimes contend that they believed that the works they were selling had been the subject of a legitimate first sale. Copyright convictions have been overturned because of inadequacies in the government's proof on this issue. See, e.g., United States v. Goss, 803 F.2d 638 (11th Cir. 1986) (reversing conviction because government failed to prove that copies were illegally made or not owned by the defendant); United States v. Atherton, 561 F.2d 747 (9th Cir. 1977) (reversing conviction because transfer of motion picture films to a salvage company constituted a first sale). For this reason, federal prosecutors should be aware of the first sale doctrine when considering whether to bring a criminal copyright case.

Since the first sale doctrine never protects a defendant who makes unauthorized reproductions of a copyrighted work, the first sale doctrine can only be a successful defense to an allegation of copyright infringement by distribution. In such instances, a defendant may argue that he or she merely *re*-distributed an otherwise authorized and legally made copy of a copyrighted work.

Moreover, the first sale doctrine may be invoked by a defendant only if he or she has been involved in the distribution of authorized copies. If copies are unauthorized, the first sale doctrine does not apply. See United States v. Drum, 733 F.2d 1503, 1507 (11th Cir.) ("Thus, where the source of copies is unlawful, the doctrine is not implicated.") (citing United States v. Moore, 604 F.2d 1228, 1232 (9th Cir. 1979) ("A pirated tape that is reproduced from the original recording without authorization is plainly not the subject of a first sale.")), cert. denied, 469 U.S. 1061 (1984); see also United States v. Powell, 701 F.2d 70, 72 (8th Cir. 1983) ("Courts have applied the first sale doctrine only where the possibility existed that the person possessing the copyrighted work obtained it lawfully in the first place."). Therefore, if B knows that the copies he or she possesses are unauthorized, B cannot defend against an infringement claim by arguing that other, unrelated copies were the subject of a first sale. For instance, in a case involving computer software programs, it may be sufficient to show that a particular program was not licensed to the individual who possessed it. Many software companies keep records of authorized licensees for just this purpose. Incidentally, it is an academic point that when a person distributes a legally acquired copy, if he or she keeps an additional copy, even a "backup" copy, this unauthorized copy can be an infringing reproduction. See supra Section III.B.2 at page 41 (discussing scope of "archival" exception codified at 17 U.S.C. § 117(a)(2)).

Further, the privileges created by the first sale principle do not "extend to 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). Most computer software is distributed through the use of licensing agreements. Under this distribution system, the copyright holder remains the "owner" of all distributed copies. For this reason, alleged infringers should not be able to establish that any copies of these works have been the subject of a first sale. Thus, if A, the copyright owner, simply loans a copy of a work to B, B obtains no ownership interest in the work and is unable to assert first sale as a defense to an infringement action. This is an important limitation, as the distribution systems for some artistic works, most notably motion pictures and computer software, rely on licensing agreements, leases, or other

devices to transfer possession of copies of a copyrighted work. Under these distribution systems, the copyright holder remains the "owner" of all distributed copies.

Although courts agree that the first sale principle applies to criminal prosecutions, they do not agree on the burden of proof. Several cases suggest that in criminal copyright prosecutions, the United States must prove that copyrighted work was not the subject of a first sale. See, e.g, United States v. Sachs, 801 F.2d 839, 842 (6th Cir. 1986) (government satisfied burden of disproving first sale with respect to videotape copies of motion pictures); United States v. Powell, 701 F.2d 70, 72 (8th Cir. 1983) (government need not allege knowledge of absence of first sale in indictment); United States v. Wise, 550 F.2d 1180, 1191-92 (9th Cir.) (government failed to carry its burden of showing that there was no first sale under agreements loaning a motion picture to actors for personal use), cert. denied, 434 U.S. 929, and rehearing denied, 434 U.S. 977 (1977); United States v. Atherton, 561 F.2d 747, 749 (9th Cir. 1977) (reversing conviction on all but one count because of deficiency in government's proof that motion picture prints were not subject to first sale); United States v. Drebin, 557 F.2d 1316, 1326 (9th Cir. 1977) (government met burden of proving that motion pictures at issue were not subject to first sale), cert. denied, 436 U.S. 904, and rehearing denied, 438 U.S. 908 (1978). Other cases, however, hold that the issue of a first sale is an affirmative defense that must be raised by the defendant. See, e.g., United States v. Larracuente, 952 F.2d 672, 673-74 (2d Cir. 1992) (holding that, as in a civil case, the government need only prove ownership of a valid copyright and unauthorized copying); United States v. Goss, 803 F.2d 638, 643-44 (11th Cir. 1986) (burden shifts to government after defendant shows that copies were legally made and that he or she owns them).[7]

Evidence of reproduction of unauthorized copies is the best and easiest way of meeting the government's burden under the "first sale" doctrine, whether it presents itself as an element or as an affirmative defense. In cases involving violation of distribution rights, two types of circumstantial proof typically demonstrate the absence of a first sale. First, when a defendant's actions indicate that copies have been obtained illegitimately, a jury may infer that no valid first sale has occurred. See United States v. Moore, 604 F.2d 1228, 1232 (9th Cir. 1979) (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) (circumstances surrounding tape sale connoted illicit origins). Factors which indicate that copies were obtained illicitly

---

[7] The legislative history of the copyright statute supports the view that the first sale doctrine was intended as an affirmative defense to copyright infringement:

> 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.

H.R. Rep. No. 94-1476, at 81 (1976), reprinted in 1976 U.S.C.C.A.N. 5659, 5695.

include: sale of copies at a price far below legitimate market value; distribution of copies of inferior quality; copies with identical serial numbers; and presence of false information on the copies, such as a false address for the manufacturer. See United States v. Drum, 733 F.2d 1503, 1507 (11th Cir.) (rebuttal of first sale defense included direct and circumstantial evidence concerning fictitious labels, low prices, and clandestine sale), cert. denied, 469 U.S. 1061 (1984); Whetzel, 589 F.2d at 712 (sale of copies of tapes from the back of a van in a parking lot).

Second, the nature of the distribution system employed by the copyright holder may negate the possibility of a first sale. For instance, the absence of a first sale has been established by showing that the works in question were distributed exclusively through loans and leases. Since the first sale defense is premised on a sale and the transfer of title, evidence that the copyright holder sold no copies of the work effectively negates this claim. Compare United States v. Drebin, 557 F.2d 1316 (9th Cir. 1977) (government proved the absence of first sale through evidence that the copyrighted movies had never been sold or transferred; 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), cert. denied, 436 U.S. 904, and rehearing denied, 438 U.S. 908 (1978), with United States v. Atherton, 561 F.2d 747 (9th Cir. 1977) (government failed to prove the absence of first sale of a number of films because, although the copyright owner never "sold" copies, it permitted ABC Television Network to permanently retain copies; these transfers fell within the definition of first sale, and ABC Television could have been the source of the movie copies sold by defendant). See also United States v. Sachs, 801 F.2d 839 (6th Cir. 1986) (evidence that defendant duplicated and sold videotaped copies of movies when the films were either not sold or sold in a different form satisfied government's burden under the first sale doctrine).

Some defendants have argued that the government must account for the distribution of all copies of a work in order to carry its burden on this question. This would require, in effect, that the government trace the distribution of every lawful copy of a copyrighted work, an unreasonable burden particularly because pirated works tend to be among the most frequently purchased and widely distributed. This argument has been consistently rejected by the courts. See, e.g., United States v. Moore, 604 F.2d 1228, 1232 (9th Cir. 1979) ("[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 ("The 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.").

3. The "fair use" doctrine in criminal cases

The equitable "fair use" doctrine, codified at 17 U.S.C. § 107, limits the exclusive rights of a copyright owner. Generally speaking, the fair use doctrine excepts the otherwise infringing use of a work where it is used for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research. Serious questions of fair use often arise in civil copyright infringement cases. The statute provides four factors that should, at a minimum, be considered when determining whether a use is a fair use: (1) the purpose and character of a use, including whether such use is of a noncommercial nature; (2) the nature of the 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 the copyrighted work.

In a criminal infringement action under 17 U.S.C. § 506(a)(1), the fair use doctrine should not, as a practical matter, impose any significant burden on the government. The prosecution is already required by 17 U.S.C. § 506(a)(1) to demonstrate willful infringement for purposes of commercial advantage or private financial gain. Proof of these elements, if sufficient, would virtually preclude any defense of non-infringing fair use in a prosecution under 17 U.S.C. § 506(a)(1). The fair use defense may be implicated, however, in prosecutions under the recently added 17 U.S.C. § 506(a)(2), which criminalizes large-scale infringement even where the infringer does not act for purposes of commercial advantage or private financial gain. See Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 451 (1984) ("[A]lthough every commercial use of copyrighted material is presumptively . . . unfair[,] . . . noncommercial uses are a different matter.").

The first factor in a fair use inquiry is the purpose and character of the use. See 17 U.S.C. § 107(1). Commercial uses are presumptively unfair, whereas for noncommercial, nonprofit activity, "[t]he contrary presumption is appropriate." Sony, 464 U.S. at 449. 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," i.e., it adds something new. "Although such transformative use is not absolutely necessary for a finding of fair use, the goal of copyright, to promote science and the arts, is generally furthered by the creation of transformative works." Id. at 579 (citation omitted). If a work is transformative, other factors which would weigh against a finding of fair use, such as the commercial nature of the use, bear less weight. See id.

The second factor for consideration 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. For example, "[t]he 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). Fair use is more difficult to establish in the case of these "core" fictional works. See Acuff-Rose, 510 U.S. at 586.

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). If the portion of the copyrighted material used is substantial or even especially important, a defense of fair use is less likely to succeed. See Harper & Row, 471 U.S. at 564-66.

Finally, courts consider the effect on the potential market for the copyrighted work or on its 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 (citation omitted). The Supreme Court has emphasized the importance of this last 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.").

Because § 506(a)(2) prosecutions typically involve piracy of commercially popular works, the last two factors should prove most useful to overcoming a fair use defense. In such cases, 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.

D. Statutory Penalty for Criminal Copyright Infringement

The penalties available for criminal infringement are codified at 18 U.S.C. § 2319. For the misdemeanor violations, a defendant may be sentenced to up to one-year imprisonment and fined up to $100,000. See 18 U.S.C. §§ 2319(b)(3), 3571(b)(5). For a felony violation, where the infringement consists of the reproduction or distribution during a 180-day period of no fewer than ten copies or phonorecords which have a total retail value of more than $2,500, the maximum penalty can be three or five years imprisonment, depending on what purpose can be proven. If the government proves that the defendant acted for purposes of commercial advantage or private financial gain, and obtains a conviction under 17 U.S.C. § 506(a)(1), the maximum sentence for a first time offender is imprisonment for up to 5 years and a fine of up to $250,000. See 18 U.S.C. §§ 2319(b)(1), 3571(b)(3). Those with a prior copyright infringement conviction are subject to up to 10-years' imprisonment. See 18 U.S.C. § 2319(b)(2). If a financial motivation is not proven in a felony case, and the conviction is obtained under 17 U.S.C. § 506(a)(2), the defendant can be imprisoned for up to 3 years – six years for the repeat offender – and fined up to $250,000. See 18 U.S.C. §§ 2319(c), 3571(b)(3).

The defendant is sentenced under U.S. Sentencing Commission, Guidelines Manual § 2B5.3 (Nov. 1998 & Supp. 2000). For detailed discussion of consequences of a conviction under 18 U.S.C. § 2319, see infra Chapter VII at page 108.

E. Novel Copyright Infringement Issues Related to the Internet

Many of the Internet's characteristics have contributed to explosive growth in copyright infringement. These characteristics include its success as a communications medium, the large number of people worldwide who use it, and the ease with which materials may be made available for copying. Media products produced today, including software and music, are often in a digital format, which permits production of copies equal in quality to the original. The digital nature of today's media products also makes them much easier to distribute in large scale to a large audience over the Internet. The ability to duplicate and distribute with near perfect quality has increased not only the amount of copying that occurs online, but the incidence of infringement. In fact, some Web sites are dedicated, either entirely or in part, to providing widespread access to copyrighted materials. These sites, commonly known as "warez" (pronounced "wayrz," or "wayrss") sites, make large quantities of commercial software available illegally – via download – to the general public.

In addition to specific sites that are exclusively dedicated to promoting infringement, specific technologies have also developed to facilitate copying via the Internet. These technological advances, in the form of software and services that make the use of software easier, will provide prosecutors with novel challenges prosecuting online intellectual property violations. The tension between copyright laws and online copying technologies is of increasing interest to the public and software programmers, some of whom may be anxious to exploit it. See, e.g., John Markoff, Cyberspace Programmers Confront Copyright Laws, N.Y. Times, May 10, 2000, at A1. While each passing month seems to bring new and more advanced technologies to the fore, a few examples will be discussed briefly below. One fact is clear, however: the Internet and related developments in technology have altered and will continue to profoundly alter the ease with which people may engage in infringing activities.

A few issues sometimes arise in particular Internet cases: (1) infringement without profit motive; (2) unusual proof issues for quantity, loss, and identity; (3) disclaimers; (4) sympathetic defendants including juveniles, and (5) novel means of infringement, including facilitation, MP3, and file sharing technologies. Each of these subjects is discussed briefly below.

1. Large scale infringement without profit motive

Infringement without profit motive is far more common in cases of Internet-based copyright infringement than it is in the physical world. Until recently, the prosecution was required to prove that copyright infringement was done willfully and for commercial advantage or private financial gain. Now the law provides for prosecution in the absence of these monetary considerations. Specifically, the current statute, as codified at 17 U.S.C. § 506(a)(2), allows for prosecution in cases involving large scale illegal reproduction or distribution of copyrighted works where the infringers act willfully, but without a discernible profit motive. Congress specifically made this change as part of the No Electronic Theft (NET) Act of 1997, Pub. L. No.

105-147, 111 Stat. 2678.[8]

In August 1999, the first person was convicted for illegally posting computer software programs, musical recordings, and digitally-recorded movies on his Web site, and allowing the general public to download and copy these products free of charge. The Oregon defendant pleaded guilty to a felony. See Ashbel S. Green, Net Piracy Law Gets First Conviction: UO Student, Portland Oregonian, Aug. 21, 1999, at A1; United States Attorney's Office, District of Oregon, First Criminal Copyright Conviction Under the "No Electronic Theft" (NET) Act for Unlawful Distribution of Software on the Internet, August 20, 1999 <http://www.cybercrime.gov/netconv.htm>. Subsequently, another person was convicted of misdemeanor copyright infringement in federal court in the District of Columbia in December 1999. See Bill Miller, Giveaways Costly for Web Pirate, Wash. Post, Dec. 23, 1999, at B1; Department of Justice, Virginia Man Pleads Guilty To Charges Filed Under the "No Electronic Theft" (NET) Act for Unlawful Distribution of Software on the Internet, Dec. 22, 1999 <http://www.cybercrime.gov/thornton.htm>. In September 2000, a Phoenix man was charged with four counts of misdemeanor copyright infringement in the Northern District of California for reproduction and distribution of the film "Star Wars Episode I: The Phantom Menace." Scott Craven, "Phantom Menace" Case May Test Laws, Ariz. Republic, Sept. 22, 2000, at B1; United States Attorney's Office, Northern District of California, For Immediate Release, September 20,

---

[8] This statutory amendment was enacted in response to United States v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994), in which a Massachusetts district court held that electronic piracy of copyrighted works, which could not be prosecuted under then-existing copyright infringement laws if the defendant did not realize a commercial advantage or financial gain, could not be charged as a wire fraud. The defendant had set up an Internet-based electronic bulletin board, to which he encouraged correspondents to upload popular software applications and computer games, which he transferred to a second encrypted address where they could be downloaded by other users with access to the password. "Although [the defendant] was at pains to impress the need for circumspection on the part of his subscribers, the worldwide traffic generated by the offer of free software attracted the notice of university and federal authorities." Id. at 536.

The defendant was charged with conspiring with "persons unknown" to violate 18 U.S.C. § 1343, the wire fraud statute. According to the indictment, LaMacchia devised a scheme to defraud that had as its object the facilitation "on an international scale" of the "illegal copying and distribution of copyrighted software" without payment of licensing fees and royalties to software manufacturers and vendors. The indictment alleged that LaMacchia's scheme caused losses of more than one million dollars to software copyright holders. Id. at 536-37. The district court explicitly recognized the wrongfulness of the defendant's conduct, but it dismissed the indictment because it concluded that Congress had "finely calibrated" the reach of criminal liability in the Copyright Act and held that "copyright prosecutions should be limited to Section 506 of the Act, and other incidental statutes that explicitly refer to copyright and copyrighted works." Id. at 545. For a more extended discussion of charging mail or wire fraud in infringement cases, see infra Section VI.B.1 at page 73.

2000 <http://www.cybercrime.gov/spatafore.htm>. Prosecutors should not hesitate to utilize this avenue of enforcement. In many cases the damage to the victim may be enormous although the infringer is not profiting financially. In fact, because the copyrighted materials are provided without charge to the entire Internet-using public, there may be enormous potential loss to the rights holder.

2. Proof issues: quantity, loss, and identity

Internet cases also raise unusual evidentiary and proof issues. One substantial challenge for Internet cases is to accurately determine the identity and quantity of the infringing items (pirated copyrighted works) that were distributed. While it may be relatively easy to determine the identity of the pirated works made available on a site, it can be a challenge to determine the identity and quantity of the works actually downloaded or distributed, unless the entity hosting the Web site keeps specific logs. For example, in order to initiate a felony copyright prosecution under 18 U.S.C. § 2319, the government must establish that at least 10 illegal copies were made during a 180-day period, with a total value exceeding $2,500.

Establishing the quantity of specific copied works is important to accurately establish a loss figure for sentencing as well. The Sentencing Guidelines now take into account some of these difficulties. For example, effective May 1, 2000, a sentencing enhancement is applicable if the defendant uploads a copyrighted work to an Internet site with the intent to allow others to download or otherwise access the infringing item. See U.S. Sentencing Commission, Guidelines Manual § 2B5.3(b)(2) (Nov. 1998 & Supp. 2000). See infra Section VII.A at page 109, for more detailed discussion of the relevant sentencing guidelines, including a discussion of determining proper valuation.

While each investigation may employ different techniques, law enforcement agencies should utilize all available resources in identifying victims and determining loss. In certain circumstances, assistance might be sought from the private sector. Certain private industry business associations, such as the Business Software Alliance, the Interactive Digital Software Association, the Motion Picture Association of America, the Recording Industry Association of America, and the Software Information Industry Association, have provided significant assistance in previous investigations. See Appendix A for a list of industry contacts.

Internet cases also involve calculating loss for purposes of restitution. Internet piracy will likely result in substantial losses to multiple victims. Since the offenders may have operated without a discernible profit motive, however, there may be few assets available to comply with a restitution order. Pursuant to 18 U.S.C. § 3663A, however, restitution is mandatory. The challenge will be to craft a reasonable means of providing restitution over the longest possible period of supervised release or probation. For additional discussion of restitution in intellectual property cases, see infra Section VII.B at page 115.

Assuming an investigation establishes that a particular Web site is a significant source of

copyright infringement, effective prosecution will also require that the government link the defendant to that Web site. Although each Web site will have a domain name, and arguably a corresponding domain name registration, it is possible and perhaps probable that much of that information will be falsified in order to shield the criminal's identity. Care must be taken to meet the burden of showing that the defendant is in fact responsible for the infringement taking place. With regard to an Internet infringement case, this will likely require a showing that the defendant maintained some form of knowing control over the content and maintenance of the subject Web site.

3. Disclaimers

Internet sites offering copies of infringing materials frequently provide so-called "disclaimers" in an attempt to immunize their operators from criminal liability by establishing a good faith defense. Although such disclaimers could conceivably be evidence of the operator's good faith, in many cases they can actually be helpful evidence of the defendant's awareness of the law, and thus be used to establishing willfulness. For example, in United States v. Gardner, 860 F.2d 1391, 1396 (7th Cir. 1988), cert. denied, 490 U.S. 1023 (1989), the Seventh Circuit rejected the defendants assertions that his disclaimer shifted responsibility to the purchaser and concluded that "such statements establish that he was well aware that his actions were unlawful." See United States v. Knox, 32 F.3d 733, 753 (3d Cir. 1994) (rejecting defendant's argument that disclaimers in brochure stating that child pornography videos were legal disproves the mens rea element and concluding that "[i]f anything, the need to profess legality should have alerted Knox to the films' dubious legality"), cert. denied, 513 U.S. 1109 (1995); see also Rice v. Palladin Enters., Inc., 128 F.3d 233, 254 (4th Cir. 1997) (observing that a jury could readily find the "For academic study only!" disclaimer in promotional sales catalogue for Hit Man book "to be transparent sarcasm designed to intrigue and entice"), cert. denied, 523 U.S. 1074 (1998); ON/TV of Chicago v. Julien, 763 F.2d 839, 844 (7th Cir. 1985) ("Whatever the attempted legal effect of the defendant's disclaimer, the ultimate trier of fact could easily find that it was a transparent attempt to deny the patent illegality of the defendant's acts. . . ."); Time Warner Entertainment/Advance-Newhouse Partnership v. Worldwide Elecs., L.C., 50 F. Supp. 2d 1288, 1296-97 (S.D. Fla. 1999) ("[C]ourts have found that a pirate decoder seller's use of such disclaimers reflects their awareness of the illegality of their business." (citing cases)); cf. Direct Sales v. United States, 319 U.S. 703, 712-13 (1943) (holding that jury may infer intent to assist a criminal operation based upon a drug distributor's marketing strategy).

4. Sympathetic defendants, including juveniles

In online infringement cases, the defendant may be young (e.g., college-age), have no criminal record, or otherwise be sympathetic to a jury. In such cases, the government should be able to provide a basis for a determination that the defendant was in fact acting egregiously and was not merely engaged in technical violations of the law. While the means of overcoming this hurdle will vary from case to case, some factors to show that the defendant was acting egregiously include establishing: (1) a significant amount of infringement; (2) the infringing

activity occurred repeatedly over a lengthy period of time; (3) the defendant was so involved in the infringement as to lead unavoidably to the conclusion that his or her actions were willful; (4) the defendant in some way profited from the conduct; (5) communications reflecting malice or other criminal intent; and (6) if applicable, some of the copyrighted works belonged to smaller companies, whose profitability may be jeopardized by the defendant's conduct.

If the defendant is a juvenile, options for federal prosecutors are limited. The federal government may proceed against juveniles in federal court for acts of juvenile delinquency other than a crime of violence or a crime involving a controlled substance only if the Attorney General – or his or her designee for these purposes – certifies that the applicable juvenile or state court has declined prosecution of the juvenile, or the state does not have available programs and services adequate for the needs of juveniles. See 18 U.S.C. § 5032. Prosecutors confronted with juvenile defendants are encouraged to review the U.S. Attorneys' Manual § 9-8.00. They should also consult any experts on juvenile prosecutions in their office. Transferring a person from juvenile status to adult status requires consultation with the Terrorism and Violent Crime Section of the Criminal Division, which can be reached by calling (202) 514-0849. Prosecutors may want to consult with attorneys from that section even if they do not seek a transfer. In appropriate circumstances, prosecutors should consider fully the option of federal prosecution. Otherwise, prosecutors should consider referring a case involving a juvenile to state authorities. See infra Section VI.A.2 at page 86 for additional discussion of state prosecution issues.

5. Challenges of emerging technology: Novel means of infringement, including facilitation, MP3, and file sharing technologies

Increasingly advanced software enables criminals to violate intellectual property rights more quickly, more frequently, and with better quality than in the past. Prosecutors may consider investigating some of the individuals who develop, utilize, and distribute these technologies. In so doing, it is essential that prosecutors understand the underlying technologies in order to appropriately differentiate lawful from unlawful conduct and to address potentially novel challenges that these technologies may present. Because the legal treatment of certain advanced reproduction technologies may be unsettled, consultation with the Computer Crime and Intellectual Property Section is strongly encouraged when evaluating these cases.

Novel means of infringement generally. The Internet facilitates infringement — particularly reproduction and distribution — in a variety of novel ways. Unauthorized copies of works may be published or posted on Web sites, or made available through other technological means. For example, they may be uploaded ("posted") to the Usenet, a group of separate bulletin boards allowing users to carry on discussions by posting questions, comments, files, and information on various topics. It is possible to copy the work to numerous Usenet bulletin boards at once ("cross-posting"). Other technological means of distributing works are sites designed merely to transfer files by means of the file transfer protocol ("FTP sites") or chat rooms for those interested in copying files, most commonly occurring on chat rooms run under the Internet Relay Chat ("IRC") protocol.

Making unauthorized copies of works available to the public for reproduction and distribution can be infringement even if it is done through a cutting edge medium such as an Internet Web site. See, e.g., Michaels v. Internet Entertainment Group, Inc., 5 F. Supp. 2d 823, 834 (C.D. Cal. 1998) (publishing copyrighted videotape on Internet Web site constitutes infringement of plaintiff's right to distribute work). To show distribution, it is not necessary to prove that others actually copied or used the work, only that the defendant knowingly made it available to the public. See Hotaling v. Church of Jesus Christ of Latter-Day Saints, 118 F.3d 199, 203 (4th Cir. 1997) (distribution occurs when all steps necessary to make a work available to the public have been completed, regardless of whether persons actually used the work).

In criminal cases, of course, copyright liability against service providers for transmitting infringing materials is limited by the government's burden of proving that the infringement was done "willfully." See infra Section III.B.3 at page 43 (discussing "wilfullness" requirement under criminal copyright infringement). Even in civil cases, courts have examined whether a bulletin board service or Internet Service Provider can be liable for infringement – whether under theories of direct or contributory infringement or, alternatively, vicarious liability – if it merely provides the means to store or transmit files that other parties upload and subsequently download. See, e.g., Playboy Enters., Inc. v. Chuckleberry Publishing, Inc., 939 F. Supp. 1032, 1040, 1044-45 (S.D.N.Y. 1996) (requiring to bulletin board system based in Italy that contained infringing images to shut down or to refrain from accepting subscriptions from customers living in the United States); Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995) (granting defendant's motion for summary judgment as to direct and vicarious copyright infringement but not as to contributory copyright infringement for provision of access to Usenet newsgroup system and Internet access server that facilitated dissemination of infringing works over the Internet where the plaintiff's raised a genuine issue of fact regarding whether the defendant had adequate knowledge after receiving a notice letter from plaintiffs). In these and similar cases, courts have attempted to differentiate between passive and active providers. Passive providers generally facilitate transfers without human intervention and without looking at the content of files which users transfer. Active providers have taken some affirmative action, such as attempting to control content of user uploads, and are therefore considered more responsible for infringement than passive providers.

Moreover, any assessment of service provider liability should also be considered in light of Congress' reaction to the issue – the enactment of the Online Copyright Infringement Liability Limitation Act, Pub. L. No. 105-304, 112 Stat. 2877 (1998), which significantly circumscribes the conditions under which online service providers might incur liability. See 17 U.S.C. § 512. This section provides limitation for infringement in four different scenarios:

- Transmissions: Automatically transmitted communications (such as electronic mail messages) that are not modified or edited by the service provider and that are not maintained any longer than reasonably necessary, 17 U.S.C. § 512(a);
- Caching: System caching of materials requested by users (such as popular Web pages) on behalf of subsequent users as long as the service provider complies with

industry standard data protocols, 17 U.S.C. § 512(b);

- Storage: Information residing on systems at the direction of users (such as a hosted Web site) as long as the service provider does not have knowledge of the infringement or financial benefit directly attributable to the infringing activity and where the service provider, upon notification, removes the infringing materials, 17 U.S.C. § 512(c); and
- Linking: Information location tools (such as a hypertext link) referring or linking users to an online location containing infringing material or infringing activity as long as the service provider does not have knowledge of the infringement or financial benefit directly attributable to the infringing activity and where the service provider, upon notification, removes the infringing materials or the access to them, 17 U.S.C. § 512(d);

Section 512 also provides a process by which copyright holders may notify service providers of allegedly infringing activities and service providers have certain duties to respond and by which injunctive or other relief may be sought. See 17 U.S.C. § 512(g)-(j). See also A&M Records, Inc. v. Napster, Inc., No. C99-05183 MHP, 2000 WL 573136, at *10 (N.D. Cal. May 12, 2000) (holding that Internet-based file sharing service does not meet requirements of "safe harbor" under 17 U.S.C. § 512(a)).

It is common that certain forms of intellectual property, such as computer software, are sold pursuant to a license that governs the use, including reproduction and distribution, of the intellectual property itself. Copyright law expressly provides that the exclusive rights of ownership may be transferred in whole or in part by conveyance. 17 U.S.C. § 201(d). Where a valid license is provided, activities such as reproduction and distribution within the scope of that license are not infringing.

Facilitation. One aspect of potential copyright infringement on the Internet is acting as a facilitator for copying. Because of the seemingly seamless nature of the Internet, a facilitator of infringement who actively encourages it can cause much more infringement than the party that provides the unprotected work for copying. Facilitation can be exemplified by "linking," or "deep linking." A link is a reference on one web page to a different web page. Often, the link takes the viewer directly to the other web page when the viewer clicks on the link. In terms of copyright infringement, the primary concern for prosecutors will be links to sites conducting illegal activity, particularly sites that allow copying of copyrighted materials ("warez sites").

One question for prosecutors will be how to address an individual who, while not illegally offering the software on his or her site, establishes a direct link to a "warez site" that is offering illegal software. While a target who illegally offers copyrighted software on a "warez site" is engaging in infringement, criminality is less clear if the copyrighted software is on another site to which the target simply links.

In these instances, the facts surrounding the activity will be critical. For example, is the

target's "warez site" effectively encouraging the infringement? Is there independent evidence, in addition to or aside from the "warez site," which suggests intent to infringe? Is there evidence of some illicit relationship between the target or the target's "warez site" and the site containing the copyrighted work to be downloaded? Further, what if the target links not to the beginning of the secondary site, but further or deeper into the site, directly to the downloadable software? This is known as "deep linking," when the link bypasses initial portions of a Web site and takes the user to a specific place within the targeted Web site. Prosecutors should consider the relative culpability of an individual who links a user directly to a copyrighted work and one who links the user to a site that offers the illegal software, possibly in addition to other legal information or services.

These questions illustrate the prosecutorial challenges posed by infringers' skillful use of links. The activity may be more analogous to the theories of contributory, or – if the requisite level of control exists – vicarious infringement (developed civilly), than direct infringement. Accordingly, given the appropriate facts and circumstances, prosecutors may wish to pursue prosecution, if at all, under an aiding and abetting theory rather than as simple infringement.

Online service providers may have potential civil liability as facilitators as well. Courts have found that service providers have infringed by reproduction if the provider knowingly copied protected works without authorization. See, e.g., Playboy Enters., Inc. v. Webbworld, Inc., 991 F. Supp. 543 (N.D. Tex. 1997) (defendant infringed by copying images from other Internet locations, creating smaller "thumbnail" versions of the images, and charging a fee to view these thumbnail images via the defendant's Web site), aff'd, 168 F.3d 486 (5th Cir. 1999); Religious Tech. Ctr v. Netcom On-Line Communication Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995) (finding possible liability for contributory copyright infringement for provision of access to Usenet newsgroup system and Internet access server that facilitated dissemination of infringing works over the Internet depending on defendant's knowledge).

In order to address online service provider liability and to remove it under certain circumstances, in 1998, the Online Copyright Infringement Liability Limitation Act was signed into law. As outlined above, it limits, in a number of online contexts, liability of service providers. Pub. L. No. 105-304, 112 Stat. 2877 (codified at 17 U.S.C. § 512). Prosecutors should be cognizant of this provision when the conduct of an online service provider is at issue. For facilitation issues, prosecutors should give special attention to 17 U.S.C. § 512(d) which limits the circumstances under which a service provider may be liable for infringement because it utilizes technologies or tools to link users to copyrighted works.

MP3 – Audio Compression Technology. One well known technology which has enhanced the public's ability to copy music is a compression technology known as "MP3." MP3, short for MPEG-1 Audio Layer 3, uses a format originally designed for video to compress audio files at a ratio of 12:1. MP3 technology takes audio signals from the original recording and compresses them into a smaller, more easily transferable format without sacrificing the quality of the sound. Because MP3 preserves the high quality of the sound recording, and is increasingly

popular among the public, portable MP3 players are being marketed for personal use. While many people utilize MP3 technology lawfully, individuals can also use this technology to sell or distribute a high volume of illegally obtained sound recordings with relative ease. See, e.g., Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1073 (9th Cir. 1999) (describing advent of MP3 digital technology and ramifications for copyright in holding that hand-held audio device that receives, stores, and plays MP3 audio files, but does not record them directly from digital music recordings, does not violate prohibitions of the Audio Home Recording Act). Moreover, applications have developed utilizing technologies such as MP3 to provide greater access to audio files on the Internet. One online service, which made MP3 files of copyrighted audio recordings available via the Internet, was sued for copyright infringement. In granting the plaintiff's motion for partial summary judgment, the court found that the defendant's conduct did not constitute "fair use." See UMG Recordings, Inc. v. MP3.COM, Inc., 92 F. Supp. 2d 349, 351-52 (S.D.N.Y. 2000) (finding liability for copying music recordings to be provided to people who own a copy where retransmission of recordings was not transformative, recordings were used in their entirety, and activity usurped market opportunity from copyright holders).

File sharing technologies. Increasingly, software-based technologies have been developed to facilitate the sharing of files with ease. For example, Napster is a well-known online service which allows individuals to access and share files, such as MP3 files, belonging to other people via the Internet. See <http://www.napster.com>. Essentially, Napster creates a community of users with files – the size of the community depends upon who is signed on at a given time. The files are not located on the Napster server, but rather on the computers of the individual users. Napster provides software to link these users together. Amid allegations of contributory and vicarious copyright infringement, Napster has been sued civilly by the recording industry. See A&M Records, Inc. v. Napster, Inc., No. C99-05183 MHP, 2000 WL 1182467, at *10 (N.D. Cal. August 10, 2000) (granting plaintiff's motion for preliminary injunction prohibiting defendant from "engaging in or facilitating others in copying, downloading, uploading, transmitting, or distributing plaintiff's copyrighted musical compositions and sound recordings protected either by federal or state law"), stayed by A&M Records, Inc. v. Napster, Inc. No. 00-16401, 2000 WL 1055915 (9th Cir. 2000); A&M Records, Inc. v. Napster, Inc., No. C99-05183 MHP, 2000 WL 573136, at *10 (N.D. Cal. May 12, 2000) (denying defendant's motion for summary judgment and concluding that Napster does not meet the safe harbor requirements of 17 U.S.C. § 512(a)).

Other technological means can provide for file sharing as well. While Napster allows user searches for MP3 files to go through a central server, another application, Gnutella, directly links individual computers utilizing the software. This direct linking software allows one to reach hundreds of Gnutella users very quickly. See, e.g., Lee Gomes, Gnutella, New Music-Sharing Software, Rattles the CD Industry, Wall St. J., May 4, 2000, at B10 (reporting that on one evening there were over 1.5 million MP3 music recordings, computer programs, and other multimedia offerings available for free via Gnutella software). Gnutella and other analogous programs continue to evolve and improve as programmers develop the software and are generally

available for free via the Internet.

Critics argue that these types of services and software compromise intellectual property rights and result in widespread infringement, be it directly or as a contributor. Supporters argue that the services may be used constructively to share many kinds of materials that are not copyrighted or are shared with the consent of the copyright holder. Moreover, supporters argue that creators of file sharing programs such as Napster and Gnutella do not control or have no control over how the public utilizes them. For example, Napster, in its terms and conditions page, asserts that it is the users of Napster, and not Napster itself, that are responsible for compliance with the law – including copyright laws. While critics challenge the sufficiency of such efforts to minimize liability, prosecutors must be aware of the often difficult questions raised by these types of programs.

Keeping pace with changing technology. The examples highlighted here represent but a few of the many new software applications and services that greatly improve the public's ability to locate and copy protected materials online. There seems little question that over time, these technologies will not only improve, but will be surpassed by more efficient, faster, perhaps more discreet applications that further enhance the ability to copy online. Some of these applications may be designed to operate at the margin of what is proper under the copyright law, or just beyond it. A key question in these developing criminal cases under these circumstances is evidence of willfulness. As these examples illustrate, however, prosecutors will need to think critically about emerging technologies, and how they operate and are used, in order to keep pace with online infringers.

IV. TRAFFICKING IN COUNTERFEIT LABELS: 18 U.S.C. § 2318

Creative works can be protected by criminal statutes aside from the Copyright Act. The most important of these is the felony provision at 18 U.S.C. § 2318, which Congress amended on July 2, 1996 as part of the Anticounterfeiting Consumer Protection Act of 1996. Pub. L. No. 104-153, 110 Stat. 1386 (1996). This Act enhances the integrity of the copyright system by specifically prohibiting trafficking in counterfeit labels designed to be affixed to phonorecords, copies of computer programs, motion pictures and audiovisual works, as well as trafficking in counterfeit documentation or packaging for computer programs. Not surprisingly, the statute relies heavily upon copyright law. For example, for purposes of 18 U.S.C. § 2318, the terms "copy," "phonorecord," "computer program," "motion picture," and "audiovisual work" have the meanings given those terms by the copyright statute at 17 U.S.C. § 101. See 18 U.S.C. § 2318(b)(3). Forms providing sample indictments and jury instructions for trafficking in counterfeit labels, 18 U.S.C. § 2318, are provided in Appendix D at page 177.

18 U.S.C. § 2318 is not a pure copyright statute, and the scope of the protections under the statute is different from the protections afforded by the Copyright Act. The predecessor to the current § 2318, for example, clearly encompassed trafficking in counterfeit labels on both copyrighted and uncopyrighted works. See United States v. Sam Goody, Inc., 506 F. Supp. 380, 386 (E.D.N.Y. 1981) (denying defendants' motions to dismiss charges of trafficking in unauthorized sound recordings). The current law continues that broad coverage, permitting a case to be proven even without evidence of copyright so long as, for example, the mail or a facility of interstate or foreign commerce is used in the commission of the offense.

Many copyright infringement crimes make use of counterfeit labels. And, in some cases, it can be easier for the government to prove the counterfeit labeling count than the copyright infringement count. For example, the counterfeit labeling crime does not require proof of infringement, i.e., actual copying or distribution; it is enough to show that the defendant was "trafficking." In addition, a counterfeit labeling case requires proof of only a "knowing" mental state, rather than a "willful" mental state. Since both crimes use the same Guidelines sections, a 18 U.S.C. § 2318 charge is an important addition to, and in some cases, alternative to, a copyright infringement charge. Prosecutors also should consider the applicability of a criminal trademark counterfeiting statute, as labels intended to be affixed to counterfeit works often carry counterfeit reproductions of federally registered trademarks. See, e.g., United States v. Akram, 165 F.3d 452 (6th Cir. 1999) (affirming conviction under 18 U.S.C. § 2318 for trafficking in counterfeit videotapes); United States v. Bao, 189 F.3d 860 (9th Cir. 1999) (upholding conviction under 18 U.S.C. § 2318 for trafficking in counterfeit computer documentation). It is also appropriate to charge 18 U.S.C. § 2318 with the other intellectual property crimes. See, e.g., United States v. Hernandez, 952 F.2d 1110 (9th Cir.) (affirming conviction under 18 U.S.C. §§ 2318-2320 for counterfeit audio cassettes and audio cassette labels), cert. denied, 506 U.S. 920 (1991); United States v. Cohen, 946 F.2d 430 (6th Cir. 1991) (affirming conviction under 18 U.S.C. §§ 2318-2319 for duplicating and distributing copyrighted movies).

A. Elements of Trafficking in Counterfeit Labels

To obtain a conviction under 18 U.S.C. § 2318, the government must prove four elements:

(1) The defendant acted "knowingly";
(2) The defendant trafficked in labels or computer software documentation affixed or designed to be affixed to a phonorecord, a computer program or other audiovisual work;
(3) The labels or documentation were counterfeit; and
(4) Federal jurisdiction is appropriate because the work is copyrighted or for other reasons.

These elements are reviewed in turn below.

1. The defendant acted "knowingly"

The first element of the crime is that the defendant "knowingly" trafficked in the counterfeit labels or other items. Thus, 18 U.S.C. § 2318 is a general intent crime. This is an easier standard to meet than the "willfully" standard required for criminal copyright infringement. Cf. infra Section III.B.3 at page 43 (discussing the "willful" standard in criminal copyright infringement cases). Indeed, in 1982, Congress modified the mens rea element of the crime by "eliminat[ing] the requirement of fraudulent intent." S. Rep. No. 97-274, at 8 (1981), reprinted in 1982 U.S.C.C.A.N. 127, 134.

2. The defendant trafficked in labels affixed or designed to be affixed to a phonorecord, a computer program or other audiovisual work or computer software documentation or packaging

The second element is that the defendant was trafficking in labels affixed or designed to be affixed to any of four categories of works: phonorecords, motion pictures, other audiovisual works, or computer software. For computer software, the government may show – as an alternative to labels – that the defendant was trafficking in documentation or packaging. Prior to its amendment, it was unclear whether 18 U.S.C. § 2318 encompassed counterfeit labels affixed to computer software, since computer software has been classified as a "literary work" under copyright law. Whelan Assoc., Inc. v. Jaslow Dental Library, Inc., 797 F.2d 1222, 1234 (3d Cir. 1986), cert. denied, 479 U.S. 1031 (1987). Since the statute has been amended, it explicitly applies to computer software. See, e.g., United States v. Bao, 189 F.3d 860 (9th Cir. 1999) (upholding conviction under 18 U.S.C. § 2318 for trafficking in counterfeit computer documentation).

"Traffic" is defined by the statute 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). It is not necessary to prove that the defendant actually transferred particular labels if it can be proven that the defendant made the labels or obtained labels with the intent to transfer them. Thus, labels seized during the search of an ongoing counterfeiting operation (whether or not they are affixed to the works) can be used to prove the offense. On the other hand, this definition of "traffic" would exclude those who knowingly acquire counterfeit articles solely for personal use. S. Rep. No. 97-274, at 9 (1981), reprinted in 1982 U.S.C.C.A.N. 127, 135.

If the items involved are counterfeit labels, the government must prove that the counterfeit labels were "affixed or designed to be affixed to" a "phonorecord . . . computer program . . . or other audiovisual work." 18 U.S.C. § 2318(a). As the prohibitions of 18 U.S.C. § 2318 include counterfeit labels "designed to be affixed" to one of these four enumerated categories of works, it is not necessary that the label actually be attached to a work. S. Rep. No. 97-274, at 9 (1981), reprinted in 1982 U.S.C.C.A.N. 127, 135 (explaining that statutory amendment was intended to close "loophole" whereby some counterfeiters had shipped only unattached labels). It is not necessary under the statute to prove this part of the element if the items involved are counterfeit documentation or packaging for computer programs.

3. The labels were counterfeit

The third element is that the labels (or packaging or documentation, in the case of computer software) were "counterfeit." A definition for counterfeit label is provided by the statute: an "identifying label or container that appears to be genuine but is not." 18 U.S.C. § 2318(b)(1). The requirement that these labels be counterfeit distinguishes this offense from the "bootlegging" or "pirating" of recordings or tapes. Counterfeit records or tapes are works that are made to appear legitimate. Bootleg or pirated records and tapes need not have a pretense of legitimacy. Under 18 U.S.C. § 2318, only trafficking in counterfeit items is prohibited. See United States v. Shultz, 482 F.2d 1179, 1180 (6th Cir. 1973) (distinguishing counterfeit from bootleg tapes). The legislative history of 18 U.S.C. § 2318 clarifies, however, that this section can be applied 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 apparent authenticity of the product. S. Rep. No. 97-274, at 9 (1981), reprinted in 1982 U.S.C.C.A.N. 127, 135. If these cases involving simulated labels raise complex questions of trademark law, prosecutors may find it helpful to consult with the Computer Crime and Intellectual Property Section.

4. Federal jurisdiction is appropriate because the work is copyrighted or for other reasons

The final element requires one of a variety of "circumstances" to establish clear federal jurisdiction:

- a federal copyright for the work to which the label is affixed (or, for a computer program, if the documentation or packaging itself is federally copyrighted);
- use or intent to use the mails or facilities of interstate or foreign commerce in the commission of the offense; or
- occurrence of the offense in a special maritime or territorial jurisdiction of the United States.

See 18 U.S.C. § 2318(c)(1)-(4). This provision was intended to expand the reach of the statute beyond the "interstate and foreign commerce" jurisdictional base of the predecessor statute. The copyright basis was specifically intended to facilitate pendent jurisdiction based upon related claims under the federal copyright law. S. Rep. No. 97-274, at 9-10 (1981), reprinted in 1982 U.S.C.C.A.N. 127, 135-36. The legislative history also explains that the statute could be applied to cases involving documentation, packaging or labels if they were affixed or designed to be affixed to "copies of copyrighted computer programs." H.R. Rep. No. 104-556, at 7 (1996), reprinted in 1996 U.S.C.C.A.N. 1074, 1080.

B. Statutory Penalty for Trafficking in Counterfeit Labels

The maximum penalty for a violation of 18 U.S.C. § 2318 is imprisonment for five years, a $250,000 fine, or both. See 18 U.S.C. § 2318(a). The defendant is sentenced under U.S. Sentencing Commission, Guidelines Manual § 2B5.3 (Nov. 1998 & Supp. 2000). For a detailed discussion of the consequences of a conviction under 18 U.S.C. § 2318, see infra Chapter VII at page 108.

V. OTHER FEDERAL CRIMINAL LAWS PROTECTING INTELLECTUAL PROPERTY

In addition to the intellectual property crimes described above, other federal criminal law is used to protect intellectual property. First, there are other intellectual property infringement crimes. Second, has been used to protect the integrity of the intellectual property system. For example, intellectual property is disseminated by cable and satellite systems. Therefore, punishment of those who traffic in devices to intercept cable or satellite signals protects the integrity of the intellectual property system. A summary of the relevant criminal law is provided below. Third, Congress has created statutory prohibitions on circumventing copyright protection systems and providing false copyright management information. These too are described below. Finally, the section reviews the provisions protecting the formalities of the copyright and patent systems.

A. Other Crimes That Protect Against Intellectual Property Infringement

In addition to the major intellectual property infringement crimes described above, Congress has enacted a few other criminal provisions that can sometimes be used against intellectual property infringement. One of these, trafficking in recordings of live musical performances, is practically an adjunct to criminal copyright infringements. Other provisions, such as prohibitions on trafficking in misbranded food, drugs or clothing, are more closely identified with consumer protection and also provide protection against infringement.

1. Trafficking in Recordings of Live Musical Performances: 18 U.S.C. § 2319A

In 1994, as part of the Uruguay Round Agreements Act, Congress enacted 18 U.S.C. § 2319A to expressly prohibit the unauthorized trafficking in recordings of live musical performances. Pub. L. No. 103-465, 108 Stat. 4974 (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.

This statute is primarily intended for use against the burgeoning trade in "bootlegged" musical recordings. Such cases might otherwise be prosecuted as criminal infringement of the copyrights in the underlying musical compositions. In passing the Act, Congress evinced its

clear intent that unauthorized trafficking in bootlegged recordings and musical compositions, when done for the purposes of commercial advantage or private financial gain, should be treated as a serious offense. The statute has been upheld pursuant to Congress' Commerce Clause authority against a recent constitutional challenge under United States v. Lopez, 514 U.S. 549, 558-59 (1995). See United States v. Moghadam, 175 F.3d 1269, 1274-1277 (11th Cir. 1999) ("The link between bootleg compact discs and interstate commerce and commerce with foreign nations is self-evident."), cert. denied, 120 S. Ct. 1529 (2000).

The statute contains three subsections, each of which protects a different right of the performing artist. Paragraph (a)(1) prohibits fixing the "sounds" or "images" of a live musical performance. "A work is 'fixed' in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration. A work consisting of sounds, images, or both, that are being transmitted, is 'fixed' for the purposes of this title if a fixation of the work is being made simultaneously with its transmission." See 17 U.S.C. § 101. But see Moghadam, 175 F.3d at 1274 (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 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, 17 U.S.C. § 506(a) and 18 U.S.C. § 2319 or, if labeled, trafficking in counterfeit labels, 18 U.S.C. § 2318. See supra Chapter III at page 34 (criminal copyright infringement); Chapter IV at page 66 (trafficking in counterfeit labels).

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. As noted above, under the definition of financial gain, that includes "receipt, or expectation of receipt, of anything of value," 17 U.S.C. § 101, barter schemes where a person fixes, transmits, or distributes a bootleg performance in return for receiving, or hoping to receive, access to fixations or transmissions of other bootlegs would clearly be illegal. For example, a concertgoer who makes bootleg tapes of an artist's performance, planning to trade them for bootleg tapes of other performances by that artist, has acted for financial gain since he or she expects to receive valuable items (i.e., other bootleg tapes) in trade. For a detailed discussion of the commercial motivation element under 17 U.S.C. § 506 and 18 U.S.C. § 2319, see supra Section III.B.5 at page 47.

The maximum penalties for a first-time violation of 18 U.S.C. § 2319A is five years' imprisonment and a $250,000 fine. Defendants who have previously been convicted under this statute may be sentenced to a maximum of ten years' imprisonment and a $250,000 fine. See 18

U.S.C. § 2319A(a). In addition, the statute provides for mandatory forfeiture and destruction of all infringing items upon a defendant's conviction. See 18 U.S.C. § 2319A(b). Copies fixed outside the United States and imported into the United States are also subject to seizure and forfeiture. See 18 U.S.C. § 2319A(c). Further, a violation of § 2319A, like §§ 2318, 2319, and 2320, is now specifically listed in 18 U.S.C. § 1961(1)(B) as a "racketeering activity" and is subject to the RICO provisions of the Organized Crime Control Act of 1970, Pub. L. No. 91-452, 84 Stat. 922 (1970). Anticounterfeiting Consumer Protection Act, Pub. L. No. 104-153, 110 Stat. 1386 (1996). For sentencing for a violation of 18 U.S.C. § 2319A, a court would use the U.S.S.G. § 2B5.3. See infra Section VII.A at page 109 (discussing application of U.S.S.G. § 2B5.3).

2. Consumer protection crimes related to misbranded consumer items

Congress has enacted certain prohibitions, such as prohibitions on trafficking in misbranded food, drugs or clothing, that are more closely identified with consumer protection and that also provide protection against infringement. For example, the Food, Drug and Cosmetics Act, which is codified at Title 21, provides for criminal penalties (misdemeanor and felony) for the introduction into interstate commerce of any misbranded or adulterated food, drug, device, or cosmetic. See 21 U.S.C. §§ 331(a) (prohibitions on misbranding), 333 (criminal penalties). The statute provides definitions for these terms. See 21 U.S.C. § 343 (misbranded food); 21 U.S.C. § 352 (misbranded drugs and devices); 21 U.S.C. § 362 (misbranded cosmetics). See also 21 U.S.C. § 841(a)(2) (prohibiting distribution of counterfeit controlled substances). (These are in addition to the prohibitions on wire and mail fraud at 18 U.S.C. §§ 1341-1343 that are familiar to federal prosecutors. See infra Section VI.B.1 at page 73.)

Likewise, the Federal Trade Commission Act, codified at Title 15, prohibits introducing into commerce mislabeled wool, fur and textile fiber products. See 15 U.S.C. § 68a (prohibiting commercial dealing in misbranded wool products); 15 U.S.C. § 69a (prohibiting commercial dealing in misbranded fur products); 15 U.S.C. § 70a (prohibiting commercial dealing in misbranded textile fiber products). It also provides for misdemeanor penalties for violations of these prohibitions. See 15 U.S.C. §§ 68h, 69i, 70i.

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, such as the Federal Trade Commission and the Food and Drug Administration to enforce those laws. Cases appropriate for civil enforcement may be referred to the enforcing 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 has a Web site at www.ftc.gov and general information telephone number at (202) 326-2222. The Food and Drug Administration has a Web site at www.fda.gov

and may be reached by telephone at 1-888-INFO-FDA (1-888-463-6322).

B. Systems of Disseminating Intellectual Property, Such as Cable Systems and Satellite Systems

Certain businesses, such as cable television and satellite broadcasting firms, serve an important role in developing systems for the dissemination of intellectual property. Five federal statutes are often used, along with a host of state statutes, to protect these systems from traffickers who sell devices that facilitate interception of the signal carrying the protected intellectual property. The five statutes are: 18 U.S.C. § 1341; 18 U.S.C. § 1343; 18 U.S.C. § 2512; 47 U.S.C. § 553; and 47 U.S.C. § 605. Each of these will be discussed in turn. Simple interception is also criminalized by 18 U.S.C. § 2511 and 47 U.S.C. §§ 553 and 605, and will not be discussed here at length.

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

Prosecutors have employed the federal mail and wire fraud statutes, 18 U.S.C. §§ 1341, 1343, to combat the assembly and distribution of devices designed to intercept encrypted cable or satellite television signals. See, e.g., United States v. Manzer, 69 F.3d 222, 226-28 (8th Cir. 1995) (sale of illegal descrambling devices that permitted the unauthorized decryption of premium channel satellite broadcasts violates federal fraud statutes); United States v. Coyle, 943 F.2d 424, 427 (4th Cir. 1991) (sale of cable television descramblers deemed 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)); United States v. Norris, 833 F. Supp. 1392, 1394-96 (N.D. Ind. 1993) (modified converter boxes used to intercept cable transmissions violate the wire fraud statute), aff'd on other grounds, United States v. Norris, 34 F.3d 530 (7th Cir. 1994). Because prosecuting intellectual property cases under the wire or mail fraud provisions can raise complex issues for intellectual property crimes, if considering such a charge, see the discussion of the mail and wire fraud statutes infra Section VI.B.1 at page 94.

2. Devices for surreptitiously intercepting wire, oral or electronic communications, 18 U.S.C. § 2512

18 U.S.C. § 2512(1)(a) prohibits an individual from sending through the mail or carrying in interstate or foreign commerce:

> any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

18 U.S.C. § 2512(1)(b) prohibits the manufacture, assembly, possession or sale of:

> any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications

with knowledge or reason to know that such device has entered or will enter the stream of commerce. The advertisement of such devices is prohibited by 18 U.S.C. § 2512(1)(c). Violation of this section may result in a fine or imprisonment for not more than five years, or both. See 18 U.S.C. § 2512(1).

Most commonly, 18 U.S.C. § 2512 is used to prosecute those individuals who possess, assemble, or sell unauthorized satellite television descramblers that enable viewers to receive premium channel broadcasts without paying a subscription fee. See, e.g., United States v. Harrell, 983 F.2d 36 (5th Cir. 1993) (affirming conviction for illegal modification and sale of Video-Cipher II systems); United States v. Lande, 968 F.2d 907 (9th Cir. 1992) (affirming conviction for illegal descrambler units modified to enable satellite dish owners to view subscription service for free), cert. denied, 507 U.S. 926 (1993); United States v. Shriver, 989 F.2d 898 (7th Cir. 1992) (reversing dismissal of action for attempted modification and sale of television descramblers); United States v. Splawn, 982 F.2d 414 (10th Cir. 1992) (affirming conviction for assembly and sale of modified satellite television descramblers), cert. denied, 508 U.S. 919 (1993).

3. Unauthorized reception of cable service, 47 U.S.C. § 553

In addition to 18 U.S.C. § 2512, Congress has prohibited the unauthorized interception of cable communications with the passage of the Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (1984) (codified at scattered sections of Titles 15, 18, 46, 47, and 50 U.S.C.):

> No person shall intercept or receive or assist in intercepting or receiving any communications service offered over a cable system, unless specifically authorized to do so by a cable operator or as may otherwise be specifically authorized by law.

47 U.S.C. § 553(a)(1). A willful violation of this section may result in a fine of $1,000 or a term of imprisonment of not more than six months, or both. See 47 U.S.C. § 553(b)(1). See United States v. Gardner, 860 F.2d 1391, 1394 (7th Cir. 1988) (affirming conviction against challenges to supposed vagueness of the statute, jury instructions on intent, and sufficiency of the evidence as to intent), cert. denied, 490 U.S. 1023 (1989). Those who willfully violate subsection (a)(1) "for purposes of commercial advantage or private financial gain" are subject to a possible term of imprisonment of two years, the penalty increasing to five years for any subsequent offense. See 47 U.S.C. § 553(b)(2). The unauthorized assembly and sale of cable television converter "descramblers" is prohibited under § 553(a)(1). See, e.g., United Sates v. Coyle, 943 F.2d 424, 426 (4th Cir. 1991) (affirming district court's finding that defendant assisted "in intercepting or receiving" cable transmissions without authorization).

4. Unauthorized publication or use of communications, 47 U.S.C. § 605

In addition, 47 U.S.C. § 605 provides felony protection for encrypted satellite cable programming and direct-to-home satellite services. A felony prosecution may be initiated under 47 U.S.C. § 605(e)(4) under the following circumstances:

> Any person who manufactures, assembles, modifies, imports, exports, sells, or distributes any electronic, mechanical, or other device or equipment, knowing or having reason to know that the device or equipment is primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite services, or is intended for any other activity prohibited by subsection (a) of this section, shall be fined not more than $500,000 for each violation, or imprisoned for not more than 5 years for each violation, or both.

Courts have consistently held that scrambled satellite transmissions fall within the reach of this section, as well as the misdemeanor provision of 47 U.S.C. § 605(a):

> No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person.

See, e.g., United States v. One Macom Video Cipher II, 985 F.2d 258, 260 (6th Cir. 1993) (statute prohibits the "unauthorized interception of traditional radio communications and communications transmitted by means of new technologies, including satellite communications"); United States v. Shriver, 989 F.2d 898, 900 (7th Cir. 1992) (unauthorized interception of scrambled television programming covered by 47 U.S.C. § 605(a)); Kingvision Pay Per View, Ltd. v. Williams, 1 F. Supp. 2d 1481, 1484 (S.D. Ga. 1998) (term "radio" includes satellite transmissions); Cablevision Sys. N.Y. City Corp. v. Lokshin, 980 F. Supp. 107, 112 (E.D.N.Y. 1997) (over-the-air pay television signals covered); Entertainment & Sports Programming Network, Inc. v. Edinburg Community Hotel, Inc., 735 F. Supp. 1334, 1338 (S.D. Tex. 1986) (holding satellite transmissions to be protected communications under 47 U.S.C. § 605(a)).

Less clear is the applicability of § 605 to punish the unauthorized interception of cable signals. Compare United States v. Norris, 88 F.3d 462 (7th Cir. 1996) (holding 47 U.S.C. § 605 inapplicable to theft of cable-borne signals) with International Cablevision, Inc. v. Sykes, 75 F.3d 123 (2d Cir. 1996) (cable signal theft governed by both 47 U.S.C. § 605 and 47 U.S.C. § 553), cert. denied, 519 U.S. 929 (1996) and Cablevision Sys. N.Y. City Corp. v. Lokshin, 980 F. Supp. 107, 112 (E.D.N.Y. 1997) (holding 47 U.S.C. § 605 applicable to cable-borne signals).

C. Systems of Copyright Management

In 1998, Congress created statutory prohibitions against circumventing copyright

protection systems and providing false copyright management information by enacting the Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified at 17 U.S.C. §§ 1201-1205). See also S. Rep. No. 105-190 (1998); H.R. Rep. No. 105-551 (1998); H.R. Rep. No. 105-796 (1998). In addition to the statute's provision of civil remedies, any violations of 18 U.S.C. § 1201 or 18 U.S.C. § 1202, may be prosecuted criminally as a felony with a maximum penalty of five years in prison if those violations are committed "willfully" and "for purposes of commercial advantage or private financial gain." 17 U.S.C. § 1204(a). Since this prohibition is relatively new, complex, and subject to numerous interrelated exceptions, prosecutors should proceed cautiously before bringing a case under either of these provisions. Moreover, since the prohibitions may place some restrictions on the ability of individuals to engage in speech-oriented activities, prosecutors should give particular consideration to any potential First Amendment concerns they might face, particularly as applied in a particular case. Cf. Universal City Studios, Inc. v. Reimerdes, 82 F. Supp.2d 211 (S.D.N.Y. 2000) (enjoining defendants from further dissemination of software used to decrypt protective code on DVD recordings despite potential First Amendment issues and holding the expressive aspect of the software to be minimal as compared with the need to protect the copyrighted work). Consultation with the Computer Crime and Intellectual Property Section is advised in exploring the issues presented by these cases.

1. Protecting copyright protection systems, 17 U.S.C. § 1201

Subject to a litany of exceptions, 17 U.S.C. § 1201 addresses circumvention of technological measures intended to protect copyrighted works.[9] Specifically, 17 U.S.C. § 1201(a)(1)(A) places a blanket prohibition on "circumvent[ing] a technological measure that effectively controls access to a work protected under" copyright law. Congress delayed implementation of this provision until October 28, 2000, to give the Librarian of Congress the opportunity to define a class of works deemed to fall outside the prohibition, a definition that is to be revisited every three years. Moreover, Congress provided numerous statutory exceptions, which cover a wide range of areas including: exempting libraries, law enforcement and intelligence activities; reverse engineering; encryption research; preventing access of minors to Internet material; accessing personally identifying information; and security testing. See 17 §§ 1201(d)-(j). Therefore prosecutors should review all of the possible exceptions as well as the determinations of the Librarian of Congress before bringing a case.

In addition to prohibiting simple acts of circumvention, Congress also prohibited the trafficking in circumvention technology. For instance, Congress prohibited trafficking in product or technology that is primarily produced (or has limited alternative commercial uses) or is marketed either to circumvent "a technological measure that effectively controls access" to

---

[9] To "circumvent a technological measure" means to "descramble a scrambled work, . . . decrypt an encrypted work, or otherwise . . . avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A).

copyrighted works, 17 U.S.C. § 1201(a)(2). Civil litigation has already been brought under this provision. Universal City Studios, Inc. v. Reimerdes, No. 00 Civ. 0277 LAK, 2000 WL 1160678 (S.D.N.Y. August 17, 2000) (finding violation of statute for posting program on the Internet to circumvent technology for encrypting copyrighted works in DVD format and ordering injunctive and declaratory relief). In addition, Congress prohibited trafficking in a product or technology that is primarily produced to circumvent "protection afforded by a technological measure" that "effectively protects" the rights of a copyright owner, 17 U.S.C. § 1201(b)(1). These provisions are subject to all of the myriad exceptions mentioned above, except for the delay of implementation and the exemption of specific works relating to determinations of the Librarian of Congress.

Similar to the other prohibitions on trafficking in circumvention technologies, Congress established prohibitions on trafficking in certain analog video equipment and products that do not comply with "automatic gain control copy control technology" or "colorstripe copy control technology." 17 U.S.C. § 1201(k)(1). Those technologies are not to be used to prevent or limit consumer copying, except in specific circumstances. 17 U.S.C. § 1201(k)(2). Many of the operative terms utilized in 1201(k) have been defined in 1201(k)(4)(E) as having, "the meanings that are commonly understood in the consumer electronics and motion picture industries" as of 1998.

2. Protecting copyright management systems, 17 U.S.C. § 1202

17 U.S.C. § 1202 provides special protection for the integrity of "copyright management information." "Copyright management information" is defined as any of eight specific kinds of information conveyed in connection with copies of a work, such as the title of the work, the name of the author, and the terms and conditions for the use of the work. 17 U.S.C. § 1202(c). First, it is unlawful to knowingly and with a deceptive intent provide, distribute, or import false copyright management information. 17 U.S.C. § 1202(a). Further, it is unlawful to intentionally remove or alter copyright management information without proper authority, or to distribute or import either works or copyright management information knowing that the copyright management information has been altered or removed without authority, or to do so knowing or having reasonable grounds to know, that doing so will lead to infringement of a protected work. See 17 U.S.C. § 1202(b). 17 U.S.C. § 1202 also contains specific exemptions for law enforcement, intelligence and other government activities. 17 U.S.C. § 1201(e). The statute also provides certain limitations on liability for certain broadcast stations and cable systems. Id.

D. The Formalities of the Copyright and Patent Systems

In addition to the prohibitions against willful infringement, the copyright and patent laws also provide for sanctions against fraudulent misuse of the intellectual property system. These provisions contain relatively minor sanctions but indicate the importance of the integrity of the formal system of intellectual property.

1. Protection of copyright notices, 17 U.S.C. § 506(c)-(d)

Although it is no longer a prerequisite to receiving protection, there are advantages to placing copyright notices on copies of copyrighted works. The purpose of 17 U.S.C. § 506(c) and (d) is to protect the integrity of these copyright notices. 17 § 506(c) provides that:

> Any person who, with fraudulent intent, places on any article a notice of copyright or words of the same purport that such person knows to be false, or who, with fraudulent intent, publicly distributes or imports for public distribution any article bearing such notice or words that such person knows to be false, shall be fined not more than $2,500.

Thus, 17 U.S.C. § 506(c) prohibits three distinct acts: (1) placing a false notice of copyright on an article; (2) publicly distributing articles which bear a false copyright notice; and (3) importing for public distribution articles which bear a false copyright notice. Any one of these acts, if committed "with fraudulent intent," violates 17 U.S.C. § 506(c). In appropriate cases, other fraud laws, such as 18 U.S.C. §§ 1341 and 1343, may also apply.

Additional protection of copyright notices is provided by § 506(d) which provides that:

> Any person who, with fraudulent intent, removes or alters any notice of copyright appearing on a copy of a copyrighted work shall be fined not more than $2,500.

Each offense is an infraction, imposing a maximum fine of $2,500. Unlike 17 U.S.C. § 506(a), which gives rise to civil as well as criminal liability, these sections proscribe conduct which is not civilly actionable. See Donald Frederick Evans & Assoc., Inc. v. Continental Homes, Inc., 785 F.2d 897, 912-13 (11th Cir. 1986) (no private right of action exists to enforce 17 U.S.C. § 506(c)).

2. False representations in copyright applications, 17 U.S.C. § 506(e)

As part of the copyright process, individuals who wish to claim statutory remedies for infringement of a work must file an application for copyright registration with the Register of Copyrights. These applications must identify the copyright claimant, explain how the claimant obtained the work, and identify and describe the work. See 17 U.S.C. § 409(1)-(11). The purpose of 17 U.S.C. § 506(e) is to protect against false copyright applications. The section provides that:

> Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by 17 U.S.C. § 409, or in any written statement filed in connection with the application, shall be fined not more than $2,500.

The government must prove that the defendant (1) knowingly made; (2) a false representation; (3) of a material fact; (4) in a copyright application or any written statement filed in connection with an application. In appropriate cases, other criminal laws, such as 18 U.S.C. § 1001, could also apply. This offense is an infraction, imposing a maximum fine of $2,500.

3. Forgery of letters patent, 18 U.S.C. § 497

Although infrequently the subject of prosecution, 18 U.S.C. § 497 prohibits forging letters patent 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.

4. False marking of patent, 35 U.S.C. § 292

In order to protect patent holders and the public, Congress enacted 35 U.S.C. § 292. This code provision creates a financial punishment for three distinct 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.

The first part of 32 U.S.C. § 292(a) protects patent holders. It prohibits an individual without the consent of the patentee from marking or using in advertising:

> 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.

The second and third paragraphs of 32 U.S.C. § 292(a) protect the public from false or misleading patent claims. Thus, an individual may not mark or use in advertising the word "patent" when the article is in fact unpatented. Nor is it lawful to mark or use in advertising the words "patent applied for" or "patent pending" when no application has been made or is not pending. 35 U.S.C. § 292(a). All three paragraphs of 32 U.S.C. § 292(a) require intent to deceive or counterfeit. Accidental or unintentional mismarking is not a violation of this code provision.

A violation of § 292 carries a fine of not more than $500 for every offense. The code permits enforcement through private infringement actions:

> Any person may sue for the penalty, in which event one-half shall go the person suing and the other to the use of the United States.

35 U.S.C. § 292(b).

VI. CHARGING AND OTHER STRATEGY CONSIDERATIONS FOR INFRINGEMENT CASES

This chapter provides guidance on strategic considerations when evaluating intellectual property infringement cases. First it discusses whether to charge an infringement case at all, including an extended discussion on whether to charge a corporation. It then provides analysis of other charges to consider, such as wire and mail fraud, RICO, and money laundering. Finally, it provides practical advice on how to charge an infringement case, and the role of a victim in putting such a case together.

A. Whether to Prosecute an Intellectual Property Crime

Generally, federal prosecutors should take into account the same considerations in determining whether to charge an intellectual property crime as they would with respect to all federal crimes. See, e.g., U.S. Attorneys' Manual § 9-27.220. Thus, the prosecutors should evaluate all the considerations normally associated with the sound exercise of prosecutorial discretion: the sufficiency of the evidence, the likelihood of success at trial, the probable deterrent effect, rehabilitative potential, and other consequence of conviction, in addition to the adequacy of non-criminal approaches. In exercising this discretion, U.S. Attorneys' Manual § 9-27.220 notes three situations in which the prosecutor may properly decline to take action despite having admissible evidence sufficient to obtain and sustain a conviction for a federal crime: when no substantial federal interest would be served by prosecution; when the person is subject to effective prosecution in another jurisdiction; or when there exists an adequate non-criminal alternative to prosecution. While individual U.S. Attorney's Offices may evaluate these factors with different standards, each of these grounds is discussed below with particular attention paid to intellectual property crimes.

1. The federal interest in intellectual property crimes

In determining the substantiality of the federal interest that would be served by a prosecution, the attorney for the government should weigh all relevant considerations, including: (1) current federal law enforcement priorities; (2) the nature and seriousness of the offense; (3) the deterrent effect of prosecution; (4) the person's culpability in connection with the offense; (5) the person's history with respect to criminal activity; (6) the person's willingness to cooperate in the investigation or prosecution of others; and (7) the probable sentence or other consequences if the person is convicted. See U.S. Attorneys' Manual § 9-27.230. The last factor (the consequences of a conviction for an intellectual property crime, including the probable sentence) is addressed at length elsewhere in this manual. See infra Chapter VII at page 108 (discussing consequences of conviction for intellectual property crimes). The other factors will be discussed below with specific attention to intellectual property crimes.

In recent years, Congress has taken an especially strong interest in intellectual property crimes as well as intellectual property law generally. As discussed elsewhere in this manual,

Congress has enacted stiffer penalties for intellectual property crimes and has made many intellectual property crimes a predicate offense under the money laundering and RICO statutes. Moreover, Congress took the unprecedented step of singling out intellectual property crimes for detailed accounting in the Attorney General's Annual Accountability Report. In enacting the Anticounterfeiting Consumer Protection Act of 1996, Pub. L. No. 104-153, 110 Stat. 1386, Congress required the Attorney General to include in the annual report, on a district-by-district basis, the following four criteria: (1) the number of open investigations. (2) the number of cases referred by the United States Customs Service; (3) the number of cases referred by other agencies or sources; and (4) the number and outcome, including settlements, sentences, recoveries, and penalties, of all prosecutions brought under sections 2318, 2319, 2319A, and 2320 of Title 18.[10]

a. Federal law enforcement priorities

The importance of intellectual property to the national economy, and the scale of intellectual property theft, led the Department of Justice to designate intellectual property crime as a "priority" for federal law enforcement. As the U.S. Attorneys' Manual recognizes, "from 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." U.S. Attorneys' Manual 9-27.230(B)(1) (comment).

Intellectual property crimes were formally designated a "priority" by Deputy Attorney General Eric Holder on July 23, 1999. Deputy Attorney General Eric Holder, Remarks at Press Conference Announcing the Intellectual Property Rights Initiative (Jul. 23, 1999) <http://www.cybercrime.gov/dagipini.html>. In announcing the Intellectual Property Rights Initiative, Deputy Attorney General Holder stated that the Department of Justice, the Federal Bureau of Investigation and the United States Customs Service had concluded that they must make investigating and prosecuting intellectual property crime "a major law enforcement priority." In making the announcement, he noted that

> [a]s the world moves from the Industrial Age to the Information Age, the United States' economy is increasingly dependent on the production and distribution of intellectual property. Currently, the U.S. leads the world in the creation and export of intellectual property and IP-related products.

---

[10] The federal interest in intellectual property is no recent or transitory development. It has been recognized since the ratification of the Constitution. See U.S. Const. art. I, § 8, cl. 8. Longtime Congressional interest in providing a sound federal basis for intellectual property law is further demonstrated by two comprehensive bodies of statutes: the Copyright Act of 1976 (codified as amended at Title 17); and the Lanham Act (codified as amended at 15 U.S.C. §§ 1051-1127). In fact, the Copyright Act in 1976 established federal preemption over state law because of the importance of a uniform federal copyright law. See 17 U.S.C. § 301.

Deputy Attorney General Holder also observed that "[a]t the same time that our information economy is soaring, so is intellectual property theft." Since intellectual property theft undermines the federally established copyright and trademark systems, it is especially appropriate that investigation and prosecution of these crimes be a federal law enforcement priority.

b. The nature and seriousness of the offense

Intellectual property crimes, like other crimes, vary in their nature and seriousness; it is therefore essential to consider each case on its own facts. Limited federal resources should not be diverted to prosecute inconsequential cases or cases in which the violation is only technical. Prosecutors may consider any number of factors to determine the seriousness of an intellectual property crime, including:

1. Whether the counterfeit goods or services present potential health or safety issues (e.g., counterfeit medications or airplane parts);

2. The scope of the infringing or counterfeiting activities (e.g., whether the subject infringes or traffics in multiple items or the infringes upon multiple industries or victims), as well as the volume of infringing items manufactured or distributed;

3. The scale of the infringing or counterfeiting activities (e.g., the amount of illegitimate revenue and any identifiable illegitimate profit arising from the infringing or counterfeiting activities based upon the retail value of the infringed item);

4. The number of participants and the involvement of any organized criminal group;

5. The scale of the victim's loss or potential loss, including the value of the infringed item, the size of the market for the infringed intellectual property that is being undermined (e.g., a best-selling software package or a famous trademark), and the impact of the infringement on that market;

6. Whether the victim or victims took reasonable measures that could have been taken to protect against the crime; and

7. Whether the purchasers of the infringing items were victims of a fraudulent scheme, or whether there is a reasonable likelihood of consumer mistake as a result of the subject's actions.

c. The deterrent effect of prosecution

Deterrence of criminal conduct is one of the primary goals of the criminal law. Experience demonstrates that many infringers will not be deterred by civil liability, which can be

treated as a cost of doing business. For example, even when a permanent injunction or consent decree is in force, they do not necessarily deter some defendants. Some defendants may respond to such civil remedies by changing the item upon which they are infringing, such as counterfeiting shirts bearing marks of Major League Baseball teams after being the subject of an injunction obtained by the National Football League. Others close shop only to quickly reopen under a different corporate identity. Criminal prosecution can better deter a violator from repeating his or her crime.

Criminal prosecution of intellectual property crimes is also important for general deterrence. Many individuals may commit intellectual property crimes not only because they can be relatively easy to commit (such as copying music) but also because the subjects believe they will not be prosecuted. Criminal prosecution plays an important role in establishing public expectations of right and wrong. Even relatively small scale violations, if permitted to take place openly and notoriously, can lead other people to believe that such conduct is tolerated in American society. While some cases of counterfeiting or piracy may not result in provable direct loss to the holder of the intellectual property right, the widespread commission of intellectual property crimes with impunity can be devastating to the value of such rights. The importance of general deterrence is easily understood with regard to counterfeiting of United States currency: even though some counterfeit bills can be "passed" without any harm to the monetary system of the United States, widespread commission of counterfeiting would be devastating to the value of the dollar. Today's brands have currency only to the extent that anticounterfeiting laws are enforced.

Vigorous prosecutions can change the counterfeiter's calculus. If individuals believe that counterfeiters will be investigated and prosecuted, they will be deterred. Industry groups representing victims of intellectual property crimes are acutely aware of their need for law enforcement protection for intellectual property. These victims will vigorously publicize successful prosecutions. The resulting public awareness of effective prosecutions can have a substantial deterrence effect.

d. The individual's culpability in connection with the offense

Intellectual property crimes are often committed by multiple individuals working in concert, such as a company that traffics in counterfeit goods or pirated software. See infra Section VI.A.4 at page 91 (discussing special considerations for cases involving corporations). The individuals in such an organization are not necessarily equally culpable. For example, a prosecutor may reasonably conclude that some course other than prosecution would be appropriate for a relatively minor participant. In considering the relative culpability of specific individuals within a group of people who commit intellectual property crimes in concert, a number of non-exclusive factors have proven helpful, including: (1) whether the person had oversight responsibility for others; (2) whether the person specifically directed others to commit the offense; (3) whether the person profited from the offense, as with an owner of a company or as with a salesperson receiving commissions; (4) whether the person was specifically aware of

the wrongful nature of the activity, as evidenced by the receipt of a warning such as a "cease and desist" letter or by a statement to collaborators admitting wrongfulness, but nonetheless continued to engage in the activity; and (5) whether the person took affirmative steps, such as creating misleading records, to deter investigation, and thereby facilitate commission of the offense. Other factors may also be relevant in particular cases.

e. The individual's history with respect to criminal activity

The subject's history with respect to criminal activity will of course be extremely fact dependent. Experience with intellectual property crime cases teaches that defendants often have a history of engaging in a pattern of fraudulent conduct not necessarily limited to intellectual property crimes. It should not be assumed that commission of an intellectual property crime is an exception to an otherwise law-abiding life. Therefore, it is appropriate to consider whether there is a reasonable basis to believe that the person has engaged in previous intellectual property violations. A prosecutor, an investigator or a victim may be aware of any permanent injunction or consent decree in any civil case against the defendant.

f. The individual's willingness to cooperate in the investigation or prosecution of others

A defendant's willingness to cooperate will depend on the individual. Nevertheless, it is important to recognize that in intellectual property cases, defendants often have a substantial capacity for cooperation, if they are in fact willing. Since intellectual property crimes often require special materials, equipment, or information, and can involve multiple participants, defendants often can provide substantial assistance. This cooperation can take at least three forms. Most commonly, a defendant might cooperate in the investigation or prosecution of others directly involved in the same criminal scheme.

Second, a defendant might also provide valuable cooperation concerning the source or destination of counterfeit goods or pirated works. For example, if a defendant is investigated for selling counterfeit watches on a retail basis, he could provide information as to the wholesaler of those counterfeit watches; the wholesaler in turn could provide information regarding the manufacturer, or about other retailers.

Third, a defendant might also provide information concerning the trafficking of counterfeit packaging materials in which counterfeit goods may be sold. This information is easy to overlook since the price of the packaging may be relatively low in comparison to the price of the goods, particularly for high-technology items. However, such information can be invaluable. For example, a defendant accused of trafficking 2,000 counterfeit computer chips for $200 each for a total of $400,000 may also have sold 10,000 counterfeit boxes for that same kind of chip at three dollars each for a total of $30,000. Though the $30,000 in box sales may seem like a small part of a $400,000 case, it can provide an important lead concerning the purchaser of the counterfeit boxes. Since the boxes serve no other purpose than to facilitate the trafficking in

counterfeit goods, a reasonable inference is that the box purchaser may also be trafficking in the counterfeit chips. Therefore, what was a simple $30,000 worth of boxes could lead to $2 million worth of counterfeit chips.

2. Whether the person is subject to prosecution in another jurisdiction

The second situation noted by the U.S. Attorneys' Manual § 9-27.220 in which the prosecutor may properly decline to take action despite having sufficient admissible evidence is when the person is subject to effective prosecution in another jurisdiction. In intellectual property cases, as in other cases, "[a]lthough there may be instances in which a Federal prosecutor may wish to consider deferring to prosecution in another Federal district, in most instances the choice will probably be between Federal prosecution and prosecution by state or local authorities." U.S. Attorneys' Manual § 9-27.240 (comment). In determining whether prosecution should be declined because the person is subject to effective prosecution in another jurisdiction, prosecutors should weigh all relevant considerations, including: (1) the strength of the other jurisdiction's interest in prosecution; (2) the other jurisdiction's ability and willingness to prosecute effectively; and (3) the probable sentence or other consequences if the person is convicted in the other jurisdiction. U.S. Attorneys' Manual § 9-27.240. See United States v. Coffee, 113 F. Supp.2d 751 (E.D. Pa. 2000) (granting defendants' motion to transfer venue on the basis of the convenience of the parties and witnesses and the interests of justice where the impecunious defendants' home and the alleged criminal operations and were in Dayton, Ohio and only five of 57 proposed government witnesses were in Philadelphia, where an undercover operation had purchased counterfeit airplane parts).

Intellectual property cases represent a rare species where a prosecutor arguably may not be able to defer to a prosecution in the location of the primary victim. For example, a individual in one state may traffic in counterfeit sports wear bearing the counterfeited mark of a sports team located in a second state, and he might do so without ever physically entering that second state. Because of the defendant's constitutional and statutory right to be tried in the state and district in which their crime was "committed," U.S. Const. art. III § 2 cl. 3; U.S. Const. amend. 6; 18 U.S.C. § 3237, a prosecutor based in that second state – the home state of the victim – arguably may not have proper venue over the counterfeiter unless it can show that the "locus delecti" of the counterfeiting took place in the second state, a determination that must be made "from the nature of the crime alleged and the location of the act or acts constituting it." United States v. Rodriguez-Moreno, 526 U.S. 275, 280 (1999).

Although this subject has not been vigorously litigated in the criminal infringement context, ordinarily that analysis turns on the locations of the actions of the defendant, rather than the district where the harm is felt. For example, in United States v. DeFreitas, 92 F. Supp.2d 272, 276-77 (S.D.N.Y. 2000), the district court found New York venue proper in a case under 18 U.S.C. § 2320 where the counterfeit Beanie Babies were shipped from China to Canada, trucked to New York and then to New Jersey because "the very nature of the offense of 'trafficking' contemplates a continuing offense, one which begins with obtaining control over the counterfeit

goods, continues with the transport, and ends with the transfer or disposal of such goods." Cf. United States v. Muench, 153 F.3d 1298, 1303 (1998) (finding venue for failure to pay child support to be proper in Florida, where victim child lived, even though Texas was where the defendant lived and where his child support checks were due); United States v. Reed, 773 F.2d 477, 483 (2d Cir. 1985) (considering factors such as the site of the criminal acts, the elements and nature of the crime, the locus of its effects, and the suitability fo the various districts for accurate factfinding and concluding that perjury in one district in a proceeding ancillary to a proceeding in another district may be prosecuted in either). See generally Donna A. Balaguer, Venue, 30 Am. Crim. L. Rev. 1259 (1993).

Thus, in intellectual property cases, it is common that the federal prosecutor will be called upon to vindicate the rights of a victim intellectual property holder based in another district, another state, or even another country. Prosecutors should therefore be cognizant that the defendant may not be subject to prosecution in the victim's district, state or nation. Federal prosecutors should also recognize that local or state authorities may not have a great interest in punishing violations of the rights of out-of-state victim intellectual property holders. By contrast, ensuring uniform and reliable national enforcement of the intellectual property laws is an important goal of federal law enforcement.

This goal takes on added significance for federal prosecutors when the victim is based in a foreign country because of the importance of intellectual property in modern international trade. With consistent enforcement of intellectual property rights, America will continue to set an example of vigorous intellectual property rights enforcement and continue to be perceived as hospitable to foreign firms that would register their intellectual property and engage in business here.

Even if the local or state authorities express a strong interest in prosecution, they may not have an ability or a willingness to prosecute the case effectively. Intellectual property cases may not be a priority for some state or local authorities. They may have limited resources to devote to intellectual property cases. For example, a particular office may not have space to store the large inventory seized from the warehouse of a counterfeiter.

Local and state authorities may also believe that since many intellectual property rights are conferred by the federal government, they do not have the ability to prosecute any intellectual property crimes. In most cases, this belief is erroneous. There is no general federal preemption of intellectual property crimes. In fact, the vast majority of states have criminal intellectual property rights statutes. The one provision for federal intellectual property preemption is for copyright infringement, 17 U.S.C. § 301, and even this preemption permits prosecution for other kinds of crime.

For example, over half of the states have enacted criminal trademark infringement statutes, which are unfair trade or "passing off" statutes. A listing of these statutes is provided in Appendix D. These crimes are not preempted by federal law. Courts have recognized that the

Lanham Act, 15 U.S.C. §§ 1051-1127, which regulates federal trademark law, "does not preempt states' ability to recognize and protect trademark rights." Keebler Co. v. Rovira Biscuit Corp., 624 F.2d 366, 372 n.3 (1st Cir. 1980) (holding that defendant was not liable in civil trademark infringement case involving soda biscuits). The Act sets a "protective floor only and does not interfere with state laws which provide additional trademark protection." Storer Cable Communications v. City of Montgomery, 806 F. Supp. 1518, 1540 (M.D. Ala. 1992) (holding that Lanham Act did not preempt ordinance prohibiting certain anticompetitive practices in cable television case).

The Lanham Act would preempt only those rare state laws that directly conflict with its provisions or purposes by permitting an erosion of trademark rights. Mariniello v. Shell Oil Co., 511 F.2d 853, 858 (3d Cir. 1975) (holding that the Lanham Act did not preempt state law protecting franchisee's gasoline dealer franchise case). See State v. Frampton, 737 P.2d 183 (Utah 1987) (holding that Lanham Act does not preempt criminal simulation statute; the purpose of the statute was to protect consumers); Barnett v. Maryland State Bd. of Dental Exam'rs, 444 A.2d 1013 (Md. App.1982) (holding that dentist's registration of term "polydontics" as service mark did not preempt State Board of Dental Examiners from acting to ban his use of advertisements containing "polydontics" on the basis that the advertisements were misleading or deceptive). See also Warner Bros. v. American Broad. Cos., 720 F.2d 231, 247 (2d Cir. 1983) (holding plaintiff's reliance on state unfair competition law to allege a tort of "passing off" not an assertion of rights equivalent to those protected by copyright in civil infringement case involving superhero parody).

A vast majority of states (over 40) have also have enacted "truth in labeling" laws or "true name and address" statutes. In states that have enacted these laws, it is illegal to manufacture, sell, distribute, or possess a variety of items and commodities, with intent to sell, re-sell, distribute, or rent, that do not bear the name and address of the manufacturer. These statutes cover a range of items – from sound recordings and audiovisual works to petroleum products and foodstuffs. See Appendix D. In many states, these laws are misdemeanors for first-time offenders. These state laws are listed by state in Appendix D.

Courts generally have determined that these "true name and address" statutes are not preempted by federal copyright law. See, e.g., Anderson v. Nidorf, 26 F.3d 100, 102 (9th Cir. 1994) (holding California's anti-piracy statute not preempted by federal copyright laws in illegal sound recording case); State v. Awawdeh, 864 P.2d 965, 968 (Wash. App. 1994) (holding Washington's statute not preempted by federal copyright law in illegal sound recording case); People v. Borriello, 588 N.Y.S.2d 991, 996 (App. Div. 1992) (holding that New York's statute not preempted by Copyright Revision Act in illegal video recording case).

Federal copyright law does provide that as of 1978, "all legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright . . . and come within the subject matter of copyright . . . are governed exclusively by [Title 17]. Thereafter, no person is entitled to any such right or equivalent right in any such work under the common law or

the statutes of any state." 17 U.S.C. § 301(a). See, e.g., Kodadek v. MTV Networks, Inc., 152 F.3d 1209, 1212-13 (9th Cir. 1998) (holding state law unfair competition claim for releasing cartoon and merchandise derived from drawings without authorization to be preempted where complaint expressly based unfair competition claim on rights granted by the Copyright Act); Kregos v. Associated Press, 3 F.3d 656, 666 (2d Cir. 1993) (holding state law unfair competition and misappropriation claims preempted when based solely on the copying of protected expression in forms).

A substantial majority of states have enacted state piracy or unauthorized duplication statutes. Over 45 such statutes are listed in appendix F at page 189. Nevertheless, courts have regularly determined that state law claims relying on misappropriation claims are preempted. See, e.g., 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); Del Madera Properties v. Rhodes & Gardner, Inc., 820 F.2d 973, 977 (9th Cir. 1987) (holding that copyright related claims of plaintiff were preempted by federal copyright law in civil infringement case involving subdivision developers).

Legislative history suggests a Congressional intent that "misappropriation" is not necessarily synonymous with copyright infringement, and that a misappropriation claim would not be preempted. See H.R. Rep. No. 94-1476, reprinted in 1976 U.S.C.C.A.N. 5659 (1976). Courts have recognized this legislative history and have afforded it some limited weight. See, e.g., National Basketball Assoc. v. Motorola, Inc., 105 F.3d 841, 850 (2d Cir. 1997) (discussing the legislative history at length and holding that a narrow "hot-news" misappropriation claim would survive preemption for actions concerning material within the realm of copyright).

Despite preemption, many states have other statutes that may be used to address cases involving violations of intellectual property rights. Courts review arguments that actions are preempted to determine whether the rights for which protection are sought may be "equivalent" to those protected by copyright law, often turning to the "extra element" test, i.e., permitting the state law claim to survive preemption if the "extra element" is "required instead of or in addition to the acts of reproduction, performance, distribution or display." National Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 850 (2d Cir. 1997); Kregos, 3 F.3d at 666. For example, state authorities may use fraud statutes in cases involving intellectual property because of the extra element of deception that need not be proven in copyright cases. See, e.g., National Basketball Ass'n, 105 F.3d at 852 n.6 (observing that state law claims involving breach of fiduciary duties or trade secret claims to not generally be preempted); Allied Artists Pictures Corp. v. Rhodes, 496 F. Supp. 408, 447 (S.D. Ohio 1980), aff'd in pertinent part, 697 F.2d 656 (6th Cir. 1982) (determining in dicta that regulation of market practices, including fraudulent licensing, to be qualitatively different from copyright).

3. The adequacy of a non-criminal alternative in an intellectual property case

Prosecutors may consider the adequacy of non-criminal alternatives when addressing an intellectual property case. Some civil remedies, including ex parte seizure of a defendant's infringing products and punitive damages, may be available for certain violations of copyright and trademark rights. 15 U.S.C. § 1116(d) (trademark remedies); 17 U.S.C. §§ 502-505 (copyright remedies). Also, for importers of trademark-infringing merchandise, the Customs Service may assess civil penalties not greater than the value that the merchandise would have were it genuine, according to the manufacturer's suggested retail price for first offenders, and not greater than twice that value for repeat offenders. These civil fines may be imposed in the U.S. Custom Service's discretion, in addition to any other civil or criminal penalty or other remedy authorized by law. 19 U.S.C. § 1526(f). The availability and adequacy of these remedies should be carefully considered when evaluating an intellectual property case.

Yet civil remedies may be futile under various circumstances. For example, intellectual property crimes are unusual because they generally are committed without the victim's knowledge, even after the fact. The victim usually has no direct relationship with the infringer – before, during, or after the commission of the crime. If a victim is unaware of a violation by a particular defendant, civil remedies generally will be unavailing. Furthermore, without criminal sanction, infringers or counterfeiters might treat the rare case of the victim's civil enforcement of its rights as a cost of doing business.

Another important factor to consider when contemplating civil remedies is that infringers may be judgment-proof. In most cases, the infringer traffics in counterfeit items worth far less than the authentic ones. By the time law enforcement identifies the unlawful activity, the value of the infringing items that the defendant has distributed often far exceeds the funds to which the defendant has access. This phenomenon is particularly common in software infringement cases, since an infringer can reproduce large numbers of high quality copies with only minimal investment. In Internet and computer bulletin board cases, a relatively modest expenditure in a personal computer and a modem can result in the reproduction and distribution of hundreds or even thousands of exact duplications of copyrighted works. In such instances, a criminal sanction may be the only meaningful deterrent.

There are a number of other circumstances where existing civil remedies may simply be an insufficient deterrent. For example, there may be cases where there have been prior unsuccessful efforts by a victim to enforce intellectual property rights against the defendant or the existence of circumstances preventing such efforts. Criminal charges may also be necessary if counterfeiting continues despite the entry of a permanent injunction or consent decree in a civil case. As these scenarios illustrate, there are numerous situations where civil remedies may not deter the infringement, particularly where the defendant regards civil penalties as a cost of doing business. Another option to keep in mind in civil cases where there is a "repeat infringer" is that the existence of a civil order may provide a basis for a petition to the court for contempt.

Finally, civil remedies may not fully capture the wrongfulness of the defendant's criminal conduct. Counterfeiting or infringement of intellectual property threatens the very integrity of

the federal intellectual property system, just as counterfeiting of currency jeopardizes the currency system. A meaningful threat of criminal prosecution is necessary to safeguard the public's confidence in intellectual property.

4. Special considerations in deciding whether to charge corporations

Corporations are often vehicles for the commission of intellectual property crimes. Trafficking any items, including infringing items, requires the reliable performance of many functions, such as: purchasing, accounting, inventory management, quality control, sales and returns. The performance of these functions on a large scale can be substantially facilitated by the organization and know-how of a business entity. A business may be especially suited to trafficking in counterfeit items if it already participates in the market for legitimate ones. For example, a business that sells legitimate goods may also sell counterfeit goods at a lower price. The organizational nature of such infringing schemes may make a RICO charge worth considering. See Section VI.B.2 at page 98 (discussing the option of charging RICO in intellectual property cases).

While every case should be evaluated on its own facts, intellectual property crimes committed by or on behalf of corporations exhibit certain typical features. These features are worth analysis against general considerations, such as the Department's guidance on Federal Prosecution of Corporations (June 16, 1999) ("Corporate Guidance"). That guidance states that to hold the corporation liable for the illegal acts of its agents, "the government must establish that the corporate agent's actions (i) were within the scope of his duties and (ii) were intended, at least in part, to benefit the corporation." Corporate Guidance § I.B. The guidance also notes that "[i]n all cases involving wrongdoing by corporate agents, prosecutors should consider the corporation, as well as the responsible individuals, as potential criminal targets." Corporate Guidance § I.B.

The guidance identifies eight factors for prosecutors to bear in mind while considering the proper treatment of a corporate target. Corporate Guidance § II.A. These factors should be considered in intellectual property cases as they are in other cases with a corporate target. Some of the factors, such as timely and voluntary disclosure of wrongdoing and willingness to cooperate, as well as specific remedial actions taken by the corporation, are particularly fact dependent. Of the other factors, a few deserve particular attention in intellectual property cases, such as: pervasiveness of wrongdoing within the corporation; the corporation's past history; restitution and remediation; collateral consequences; and non-criminal alternatives. These are discussed individually below.

Pervasiveness of wrongdoing within the corporation. The Department's guidance recognizes that "[c]harging a corporation for even minor misconduct may be appropriate where the wrongdoing was pervasive and was undertaken by a large number of employees, or by all the employees in a particular role within the corporation, e.g., the salesmen or procurement officers, or was condoned by upper management." Corporate Guidance § IV.A. In some cases where an

intellectual property crime is committed by individuals through a corporation, the involvement can be pervasive throughout the corporation and condoned by management. For example, the sales people sell some of the company's goods at a discount to the rest of the market; the quality control team ensures that the infringing item will "pass"; the inventory manager keeps the infringing item separate from legitimate ones; and the purchaser must seek out, obtain and earmark the infringing goods obtained at a discount. It would be difficult for a "rogue" salesman to sell counterfeit items without the cooperation of the purchaser in obtaining them and the inventory manager in making their availability for sale known to him. If the counterfeit or pirated item is created in-house, then involvement is even greater: the purchaser must obtain raw materials but not the finished product; the warehouse people must assemble the item; the accountant must keep track of the adjustment to the company's inventory; and others may even be called upon from time to time to help in the warehouse. All of this participation usually takes place with the awareness and at the direction of management, as would almost be required for so pervasive a scheme.

The corporation's past history. As the Department's guidance notes, a corporation "is expected to learn from its mistakes." Corporate Guidance § V.B. Of course prosecution may be appropriate if the corporation has not responded appropriately to previous non-criminal guidance, warnings, sanctions, or criminal charges. In intellectual property cases, guidance or warnings may often be in the form of a "cease and desist" letter sent by the victim, possibly followed by initiation of civil suit. In addition, it is often the case that an infringing corporation becomes aware of contemporaneous sanctions against a similarly situated firm, such as a supplier or a competitor. Corporations may be expected to learn from the mistakes of others with whom they associate. Prosecution may be appropriate if a corporation became aware of actions against associates and yet continued to engage in the conduct at the root of the enterprise. On the other hand, declination may be justified if a corporation became aware of actions against associates and took remedial actions, such as implementing a corporate compliance program, improving an existing one, disciplining or terminating wrongdoers or management, paying restitution, or cooperating with relevant government agencies.

Restitution and remediation. In prior intellectual property cases, corporate defendants have paid substantial fines and restitution. These sanctions not only deter and punish wrongdoers, they also aid in making the victim whole. A corporation may be more likely to be able to pay substantial amounts than an individual. Of course, as the Department's guidance notes, "neither a corporation nor an individual may avoid prosecution merely by paying a sum of money." Corporate Guidance § VIII.A.

Collateral consequences. While the Department's guidance notes that prosecutors may consider collateral consequences of a corporate criminal conviction, it also recognizes that unknowing people, such as officers, directors shareholders and employees, might be affected by a corporate conviction. Corporate Guidance § IX.B. In intellectual property cases involving corporations committing infringement crimes, the illicit conduct can be pervasive throughout the corporate entity. Where these entities are closely held, few unknowing innocent people would

suffer substantial consequences. The Department's guidance also draws attention to non-penal sanctions that may arise, such as debarment from eligibility from certain government programs including government contract eligibility. Corporate Guidance § IX.B.

For example, there have been notorious cases of the government purchasing infringing items, such as airplane parts or computer chips to control satellite or military equipment, from government contractors. Under a "low bid" system, the government may be particularly susceptible to purchasing infringing goods. In cases such as these, the potential for debarment as a consequence of prosecution should be seriously considered.

Non-criminal alternatives. As discussed, prosecutors may consider the non-criminal alternatives to prosecution when addressing an intellectual property case. See supra Section VI.A.3 at page 89 (discussing non-criminal alternatives in intellectual property cases). This inquiry is equally important when the defendant is a corporation. As the Department's guidance recognizes, prosecutors may consider whether non-criminal alternatives adequately deter, punish and rehabilitate a corporation that has engaged in wrongful conduct. The Department's guidance suggests that prosecutors may also evaluate the "regulatory authority's ability and willingness to take effective enforcement action." Corporate Guidance § X.B. For the closely held corporations that are typically engaged in the commission of intellectual property crimes, there is no willing or able regulatory authority, such as the Securities and Exchange Commission, to provides oversight. Therefore, the only alternative to criminal enforcement in these cases may be a civil suit brought by the victim. This alternative is subject to many of the same concerns when dealing with a corporate target as described above for a natural target. See supra Section VI.A.3 at page 89 (discussing non-criminal alternatives in intellectual property cases).

B. Other Federal Offenses to Consider in Relation to Intellectual Property Infringement Cases

In addition to the intellectual property statutes discussed above, there are other criminal statutes prosecutors may charge in developing intellectual property cases. Of these, prosecutors should be particularly aware of the various wire and mail fraud, money laundering, and RICO statutes which are discussed below.

Prosecutors may, for the usual strategic reasons, wish to bring accessory charges, such as aiding and abetting, 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). Of course, a jury's inability to reach a verdict on an ancillary charge, such as an accompanying conspiracy count, does not necessarily affect a finding of guilt on the substantive count or counts. See United States v. Steele, 785 F.2d 743, 750 (9th Cir. 1986) (affirming conviction for copyright infringement despite dismissal of conspiracy to infringe charges).

Some crimes that are technical violations of the copyright or counterfeiting provisions

may be core violations of other provisions. For example, the computer hacker who exceeds authorization in a computer system and copies sensitive data for financial gain may be more appropriately charged under 18 U.S.C. § 1030(a)(2), whereas a person who copies trade secret information may be subject to punishment under the Economic Espionage Act, 18 U.S.C. §§ 1831, 1832. For further discussion of prosecution of trade secrets, see infra Chapter VIII at page 124.

Infringing articles are often manufactured overseas and then shipped into the United States for distribution. Commercial importation of unauthorized copies of copyrighted works constitutes copyright infringement. See 17 U.S.C. §§ 501(a), 602. If significant customs duties were avoided by counterfeiting the goods, prosecutors may consider also charging the defendant with entering goods into the United States by false statements, 18 U.S.C. § 542; or with smuggling goods, 18 U.S.C. § 545.

Absent exceptional circumstances, prosecutors considering intellectual property crimes – especially copyright crimes – should not charge interstate transportation of stolen property, 18 U.S.C. § 2314. In 1985, the Supreme Court reversed a conviction for the interstate transportation of copyrighted Elvis Presley records, holding that it was not Congress's intention that section 2314 function as a criminalization of copyright infringement. See Dowling v. United States, 473 U.S. 207 (1985). The Court reasoned that an infringer of a copyright 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. The same reasoning could apply to infringement of a trademark, which requires neither physical control nor deprivation to the owner. Moreover, trademark, like copyright is protected by an extensive body of federal law. Therefore, prosecutors should generally reserve charging § 2314 for theft of physical property and avoid using it for theft of intellectual property.

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

In many intellectual property cases, prosecutors should consider charging mail or wire fraud in addition to, or in lieu of, an intellectual property crime. Federal prosecutors, of course, need no introduction to the wire or mail fraud statutes. See, e.g., Peter J. Henning, Maybe it Should Just Be Called Federal Fraud: The Changing Nature of the Mail Fraud Statute, 36 B.C. L. Rev. 435 (1995); Jed S. Rakoff, The Federal Mail Fraud Statute (Part I), 18 Duq. L. Rev. 771 (1980).

Intellectual property cases are not removed from the reach of wire or mail fraud statutes merely because the property at issue is intangible. In 1987, the Supreme Court issued two separate opinions defining the scope of mail and wire fraud statutes in cases involving the theft of intangible property. In United States v. McNally, 483 U.S. 350 (1987), the Court rejected the view that the mail fraud statute then in effect reached schemes that denied the public the loyal services of government officials. Relying on the legislative history of these statutes, the Court

interpreted 18 U.S.C. § 1341 as "limited in scope to the protection of property rights." Id. at 360. (In response to the McNally decision, Congress enacted 18 U.S.C. § 1346 broadening the definition of a "scheme or artifice to defraud" to include "a scheme or artifice to deprive another of the intangible right of honest services.")

Read broadly, McNally might be construed to preclude all prosecutions for schemes to defraud individuals of intangible property like copyrights. Nevertheless, in Carpenter v. United States, 484 U.S. 19 (1987), the Court made clear that a scheme to defraud the owner of another type of intangible property – confidential information – was covered by the mail and wire fraud statutes. Distinguishing McNally, the Court stated that confidential business information had "long been recognized as property." Id. at 26. According to the Court, this intangible interest had received greater legal recognition as property than had the right to honest and faithful services by public employees, a right which the Court characterized as "an interest too ethereal in itself to fall within the protection of the mail fraud statute." Id. Since intellectual property has been no less recognized as property, than as confidential business information, it should be equally protected under the wire and mail fraud statutes. See generally Pamela Samuelson, Information as Property: Do Ruckelhaus and Carpenter Signal A Changing Direction in Intellectual Property Law?, 38 Cath. U. L. Rev. 365 (1989).

a. Possible advantages of charging wire or mail fraud

Charging wire or mail fraud in an intellectual property case may have several strategic advantages for federal prosecutors. Prosecutors may be more comfortable with the familiar statute. Moreover, juries may believe that fraud is less exotic and more inherently wrongful than an intellectual property crime. This is particularly true where the facts involve deception or defrauding of consumers by counterfeit merchandise, such as counterfeit automobile parts. Prosecutors should also consider the sentencing advantages, if any, of charging wire or mail fraud, although many of these comparative advantages have been eliminated with the May 1, 2000 of the Sentencing Guidelines. See infra Section VII.A at page 109.

b. Possible disadvantages of charging wire or mail fraud

Prosecutors should be wary, however, of the possible snares in charging wire or mail fraud either in addition to or in lieu of an intellectual property crime. A wire and mail fraud charge generally requires proof of a scheme to defraud, and an intent to defraud. An infringement charge would require neither.

Need for a scheme to defraud. One interesting question is whether the government may even charge fraud for pure infringement in the absence of evidence of any misrepresentation or scheme to defraud. In one copyright case, a charge of wire fraud was dismissed where no misrepresentation was alleged. 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. Compare 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.") with Aaron D. Hoag, Note, Defrauding The Wire Fraud Statute: United States v. LaMacchia, 9 Harv. J.L. & Tech. 509, 514 (1995) (criticizing the opinion as "an exercise in misdirection and obfuscation").[11]

To prove mail or wire fraud in any jurisdiction the government must establish a scheme to defraud. While the code provides no direct guidance as to what constitutes a "scheme or artifice to defraud," decisions interpreting these statutes frequently emphasize false or misleading statements made by the defendant to the victim. See McNally v. United States, 483 U.S. 350, 358 (1987) ("[T]he words 'to defraud' commonly refer 'to wrongdoing one in his property rights by dishonest methods or schemes,' and 'usually signify the deprivation of something of value by trick, deceit, chicane or overreaching.'") (citation omitted); United States v. Morris, 80 F.3d 1151, 1160 (7th Cir. 1996) (noting that statute "encompasses fraudulent schemes premised on false statements or factual misrepresentations"); United States v. Brien, 617 F.2d 299, 307 (1st Cir. 1980) (describing a "plan to deceive persons as to the substantial identity of the things they are to receive in exchange") (citation omitted). Courts have upheld fraud convictions even when the victim of the fraud had no direct contact with the perpetrator of the fraud, broadly characterizing the nature of the fraudulent conduct to fit within the language of the federal fraud statutes. See United States v. Christopher, 142 F.3d 46, 54 (1st Cir. 1998) (holding that even though injury fell on third party, fraudulent representations to insurance regulators constituted violation of the wire fraud statute since "[n]othing in the mail and wire fraud statutes requires

---

[11] The LaMacchia opinion may have significant limits. The indictment in LaMacchia did not charge the defendant with making any misrepresentations whatsoever. When there is some evidence of misrepresentation or fraud, the fact that the goods at issue were intellectual property should not bar a mail or wire fraud prosecution; Dowling does not provide contrary authority. See Cooper v. United States, 639 F. Supp. 176, 180 (M.D. Fla. 1986) (rejecting contention that Dowling precluded any mail and wire fraud prosecutions of copyright infringers who had distributed pirated eight-track and cassette tapes and were charged with "fraudulently represent[ing] to the public and to others that certain sound recordings 'were produced by the manufacturers identified on the labels of said products' when, in fact, the products were not legitimately or lawfully reproduced"); United States v. Wang, 898 F. Supp. 758, 760-61 (D. Colo. 1995) (holding that defendant's unauthorized transmission by wire of copyrighted computer files could be prosecuted under the wire fraud statute and rejecting the claim that Dowling limits the reach of the mail and wire fraud); see also Dowling v. United States, 473 U.S. 207, 209 n.l (1985) (declining to consider sua sponte the fact that the defendant did not challenge his conviction under the mail and wire fraud statutes).

that the party deprived of money or property be the same party who is actually deceived"); 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 that permitted the unauthorized decryption of premium channel satellite broadcasts violated federal fraud statutes); United States v. Coyle, 943 F.2d 424, 427 (4th Cir. 1991) (holding a 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 McNally, 483 U.S. at 358). Nevertheless, in the absence of strong evidence of misrepresentation, a prosecutor may prefer not to proceed with a wire or mail fraud charge if an infringement crime may be charged.

By contrast, fraud on the purchaser is not an element in any of the intellectual property crimes. Courts have not accepted claims by defendants that the infringement offenses with which they were charged had not been completed because no purchaser was defrauded. See, e.g., United States v. Gantos, 817 F.2d 41, 43 (8th Cir. 1987) (upholding trademark counterfeiting conviction where the defendant told the buyer that the goods were counterfeit).

Need for a specific intent to defraud. Defendants in intellectual property cases have tried to excuse their actions by stating that they did not intend to defraud the recipients of the infringing materials. Proof of specific intent to defraud is required for mail and wire fraud, but not for the infringement crimes. Where the evidence to show a specific intent to defraud is not overwhelming, a prosecutor might consider charging the case as an infringement and using the limited evidence of the defendant's fraud as part of the context for the case.

Many cases recognize that mail and wire fraud prosecutions require proof of a specific intent to defraud. United States v. Beech-Nut Nutrition Corp., 871 F.2d 1181, 1195-96 (2d Cir. 1989) (citing cases) (affirming conviction for offenses stemming from a conspiracy to sell misbranded and adulterated apple juice in interstate commerce while observing that "a finding of conscious avoidance could not alone provide the basis for finding purpose or for finding intent as a whole"). See also United States v. Gabriel, 125 F.3d 89, 98 (2d Cir. 1997). Although some cases note that reckless disregard of the truth is sufficient to prove "specific intent" in the context of mail and wire fraud, the conduct in question manifested a clear specific intent to defraud. See, e.g., United States v. Coyle, 63 F.3d 1239, 1243 (3d Cir. 1995) (health care fraud); United States v. Reddeck, 22 F.3d 1504, 1507 (10th Cir. 1994) (fraudulent correspondence university scheme); United States v. Gay, 967 F.2d 322, 326 (9th Cir. 1992) (fraudulent direct marketing scheme); United States v. Simon, 839 F.2d 1461, 1470 (11th Cir. 1988) (fraudulent oil and gas lease scheme).

The "good heart" excuse has not been accepted by the courts in intellectual property cases because none of the intellectual property crimes discussed above, 18 U.S.C. §§ 2318-2320, requires a specific intent to defraud. For example, trademark counterfeiting under 18 U.S.C. § 2320 requires only general intent, i.e., that the defendant knowingly trafficked in a counterfeit mark. One court specifically rejected a "good heart" defense that the counterfeit marks were used so that the end user could reorder authentic parts and use authentic repair manuals. See

United States v. Brooks, 111 F.3d 365, 372 (4th Cir. 1997) (affirming conviction of defendants for fraud, trafficking in counterfeit goods, and other charges in connection with sales of electrical components to the U.S. Navy). See also United States v. Gantos, 817 F.2d 41, 43 (8th Cir. 1987) (affirming trademark counterfeiting conviction where the defendant told the buyer that the goods were counterfeit). Even the "willful" mens rea required to prove criminal copyright infringement does not require the government to show a specific intent to defraud. See supra Section III.B.3 at page 43 (discussing willfulness element needed for copyright infringement prosecution).

2. RICO, 18 U.S.C. §§ 1961-1968

Prosecutors in certain intellectual property cases may consider bringing charges under the Racketeer Influenced and Corrupt Organizations (RICO) provisions found at 18 U.S.C. §§ 1961-1968. 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 predicates for a racketeering charge under 18 U.S.C. § 1961(1)(B). Recognizing the frequency with which intellectual property crimes are committed by organizations, Congress specifically added the four above-noted intellectual property crimes as predicate acts when enacting the Anticounterfeiting Consumer Protection Act of 1996. Pub. L. No. 104-153 § 3, 110 Stat. 1386 (1996). The legislative history highlights testimony from Leonard Walton, Deputy Assistant Commissioner of Investigations for the United States Customs Service, comparing the pattern of criminal activity and organizational structure associated with counterfeiting to that of drug trafficking. He then went on to explain that the RICO provisions of the law were "essential to allow law enforcement agents to take down the entire criminal organization rather than merely react to each crime the organization commits." H.R. Rep. No. 104-556, at 304 (1996), reprinted in 1996 U.S.C.C.A.N. 1074, 1075. Cf. Toms v. Pizzo, 4 F. Supp.2d 178, 184 (W.D.N.Y. 1998) (noting that §§ 2318, 2319, and 2320 are predicates for RICO).

Many large-scale infringement cases involve a regular pattern of coordinated activity by a highly structured organization, such as a corporation. See supra Section VI.A.4 at page 91 (discussing charging corporations in intellectual property cases). Thus, infringement cases may make good candidates for bringing a RICO charge. Of course, a RICO charge can add complexity to a case, and requires prior approval from the Organized Crime and Racketeering Section of the Criminal Division. U.S. Attorneys' Manual §§ 9-110.101, 9-110.320. The U.S. Attorney's Manual provides that a RICO charge should be added only if it would serve a specific consideration for a case. U.S. Attorneys' Manual § 9-110.310 (enumerating considerations). Of the enumerated considerations, two are typically of special interest in infringement cases: (1) a RICO prosecution would provide the basis for an appropriate sentence in a way that prosecution only on the underlying intellectual property charges would not; and (2) use of RICO would provide a reasonable expectation of forfeiture which is proportionate to the underlying criminal conduct.

For sentencing purposes, a RICO charge provides a minimum base offense level of 19.

See U.S. Sentencing Guidelines Manual § 2E1.1. This floor could provide an appropriate minimum sentence that would recognize the wrongfulness of, and the need to deter, such large scale criminal activity even if the entire scope or scale of the infringing activity cannot be proven. Such a floor may also help address the many difficult valuation issues that arise in sentencing infringement crimes, even with the recent amendments to the sentencing guidelines. See infra Section VII.A at page 109 (discussing sentencing for infringement crimes). Intellectual property crimes can take place without the victim rights holder ever becoming aware. Therefore, it can be difficult, once the crime is discovered, and investigated, to determine precisely how long it has been ongoing. In most cases, the scope of the crime is determined by the defendant's records or the defendant's admissions, which can be remarkably incomplete. This concern is exacerbated by the ease with which large-scale intellectual property crimes can be committed. For example, a Web site that offers downloads of copyrighted software can provide thousands of copies if it can provide one. Though less dramatically, trademark crimes can be committed on a large scale constrained only by the supply of the "knockoff" goods and the difficulty of generating the counterfeit mark.

A structured organization that engages in intellectual property infringement as a profitable and repeated practice may be a highly capital-intensive business with substantial proceeds. Such proceeds would be ripe for forfeiture, except that, as discussed separately, forfeiture provisions provided for in a pure intellectual property case are more limited than the general forfeiture provisions. See infra Section VII.C at page 120 (discussing forfeiture for infringement crimes). Unlike intellectual property crimes, RICO has broad forfeiture provisions. See 18 U.S.C. § 1964. In some intellectual property cases, a RICO charge may thereby provide a reasonable expectation of forfeiture proportionate to the underlying infringing conduct.

Prosecutors with questions concerning RICO practice should contact the RICO expert in their office or the Criminal Division's Organized Crime and Racketeering Section at (202) 514-3595. As noted above, a RICO charge can add complexity to a case, and requires prior approval from the Organized Crime and Racketeering Section of the Criminal Division. If the charge is well-grounded and clearly explained, this approval requirement should not be an undue burden to prosecutors.

3. Money laundering, 18 U.S.C. §§ 1956, 1957

Prosecutors may consider bringing additional charges under the money laundering statutes found at 18 U.S.C. §§ 1956, 1957. The penalties for a violation of these statutes can be greater than for an intellectual property violation alone. The sentencing guidelines for money laundering start at a base offense level of 17, 20, or 23; all of these are substantially greater than those for an intellectual property violation. U.S. Sentencing Guidelines Manual §§ 2S1.1, 2S1.2. A money laundering charge also provides a basis for criminal forfeiture of property involved in the money laundering offense, an option not ordinarily available in simple intellectual property cases. See 18 U.S.C. § 982(a)(1).

Criminal copyright infringement, 18 U.S.C. § 2319 and trademark counterfeiting, 18 U.S.C. § 2320 (but not counterfeit labeling, 18 U.S.C. § 2318) are specified unlawful activities that may be used as predicates for money laundering charges. See 18 U.S.C. § 1956(b)(7)(D). For example, in one recent case, the defendant had mass-produced counterfeit audio cassette recordings of releases by performers of popular music. Along with co-conspirators, he infringed the copyrights of the performers and used the proceeds from sales to expand operations. He pleaded guilty to conspiracy, copyright infringement, trafficking in counterfeit labels, and money laundering. United States v. Khalil, No. CR. A. 95-577-01, 1999 WL 455698 (E.D. Penn. June 30, 1999).

Defendants in intellectual property cases commonly violate the money laundering laws. They might violate 18 U.S.C. § 1956(a)(1) by engaging in financial transactions involving proceeds of their specified unlawful activity with the intent to promote the carrying on of further specified unlawful activity. For example, an individual who traffics in counterfeit goods may deposit the proceeds of his sales into a bank account and then use the proceeds to purchase more counterfeit goods for the purpose of trafficking. In addition, a defendant might violate 18 U.S.C. § 1957 by knowingly engaging in a monetary transaction in property of a value greater than $10,000 derived from a criminal offense that is a specified unlawful activity, such as the sale of counterfeit goods. Since these scenarios, which constitute technical money laundering violations, are so typical, it may be difficult to decide whether a particular case is appropriate for charging money laundering, particularly if the defendant is also trafficking in legitimate goods. While each case must be decided upon its own facts, certain factors have proven helpful for prosecutors in intellectual property cases considering a money laundering charge: (1) the gross amount derived from a specified unlawful activity; (2) whether the total monetary value is more than de minimis; (3) whether more than 50 percent of the funds contained in, or related to, a commingled bank account are proceeds of the specified unlawful activity and are used to promote the carrying on of further specified unlawful activities; (4) whether covert accounts, such as off-shore bank accounts, were used to conceal the activity; and (5) whether financial records were designed to conceal the use of the proceeds, such as using two sets of financial books.

Prosecutors should be aware that in so-called "receipt-and-deposit" cases, i.e., any case in which the conduct to be charged as money laundering consists of the deposit of proceeds of specified unlawful activity into a domestic financial institution account that is clearly identifiable as belonging to the person or persons (including the business entity outwardly involved in the criminal conduct) who committed the specified unlawful activity, no indictment or complaint may be filed without prior consultation with the Asset Forfeiture and Money Laundering Section. See U.S. Attorneys' Manual § 9-105.330(4). For a detailed discussion of the elements of money laundering and for Department of Justice policy, see U.S. Attorneys' Manual § 9-105.000 and Money Laundering Section, U. S. Department of Justice Money Laundering Federal Prosecution Manual (June 1994). Prosecutors with questions concerning money laundering practice should contact the money laundering expert in their office or the Criminal Division's Asset Forfeiture and Money Laundering Section at (202) 514-1263.

C. How To Charge a Copyright or Trademark Crime

1. Units of prosecution

Because a defendant often traffics in numerous labels of copyrighted works, infringes numerous copyrighted works or counterfeits numerous trademarks, it is not always easy to draft an indictment that accurately reflects a defendant's actions. The United States Department of Justice Criminal Resource Manual 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." U.S. Attorneys' Manual § 9-215.00 ("Criminal Resource Manual") (recommending charging no more than fifteen counts).

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. Prosecutors may consider charging counts by the mark or copyright infringed, by the identity of the copyright holder or mark holder, or by the date upon which the infringing goods were manufactured, distributed, or seized. Indictments charging counterfeiting and piracy schemes can be unified through a conspiracy count under 18 U.S.C. § 371.

In cases where the defendant infringed only one type of the same copyrighted work or trademark, the defendant should be charged with a single count. This amounts to counting the number of illegal copies made or distributed by the defendant in the requisite period if any and charging them as a single count in the indictment. Although no court has addressed this issue in the copyright context, it should not be held duplicitous to charge a single count of copyright infringement that alleges infringement by both "reproduction" and "distribution" because the offense is "infring[ing] a copyright," 17 U.S.C. § 506(a) and "reproduction" and "distribution" are alternate means of infringing a copyright because they are defined by the statutory scheme as alternative ways to violate the copyright holder's exclusive rights. See 17 U.S.C. § 501(a) (defining infringement as violation of an exclusive right provided by 17 U.S.C. §§ 106-118); see also 17 U.S.C. § 106(1) (exclusive right of reproduction); 17 U.S.C. § 106(3) (exclusive right of distribution). See generally, e.g., United States v. Cornillie, 92 F.3d 1108, 1109 (11th Cir. 1996) (count of indictment charging defendant with multiple means of intimidation not duplicitous because statute recited each means of committing offense). Although charging infringement by reproduction and distribution under some circumstances does permit greater penalties than other means of infringement, see 17 U.S.C. § 506(a)(2); 18 U.S.C. §§ 2319(b)(1), (c)(1), and thus it may be duplicitous to charge them in the same count with other forms of infringement, it should not be held duplicitous to charge those two means of infringement togther. See, e.g., United States v. Hixon, 987 F.2d 1261, 1265 (6th Cir. 1993); United States v. Burton, 871 F.2d 1566, 1573 (11th Cir. 1989); United States v. Uco Oil Co., 546 F.2d 833, 838 (9th Cir. 1976), cert. denied, 430 U.S. 966 (1977).

Indeed, the criminal statutes permit multiple copyrighted works to be charged in a single copyright infringement count or multiple trademarks to be charged in a single counterfeiting count. For example, the criminal copyright statute does not require that all the copyrights infringed be in the same class or even be held by the same copyright owner; a defendant may still be convicted of a felony for reproducing or distributing a total of ten copies of potentially different copyrighted works, so long as they are of the required value and the copies were made within the specified time frame. See 17 U.S.C. § 506(a)(2), 18 U.S.C. § 2319(c)(2). As the legislative history specifically notes:

> the phrase "of one or more copyrighted works" is intended to permit aggregation of different works of authorship to meet the required number of copies and retail value. For example, a defendant's reproduction of 5 copies of a copyrighted word processing computer program having a retail value of $1,300 and the reproduction of 5 copies of a copyrighted spreadsheet computer program also having a retail value of $1,300 would satisfy the requirement of reproducing 10 copies having a retail value of $2,500, if done within a 180-day period.

H.R. Rep. No. 997, 102 Cong. 2d Sess., at 6 (1992), reprinted in 1992 U.S.C.C.A.N. 3569, 3574 (1992).

The indictment may also contain separate counts for each separate copyrighted work or each separate genuine mark. For example, in United States v. Song, 934 F.2d 105 (7th Cir. 1991), a case involving counterfeit watches and handbags, 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 based its determination on the plain language of 18 U.S.C. § 2320 which covers 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 (emphasis in original). When a defendant meets the felony minimum by reproducing one class of copyrighted materials (e.g., 10 copies of a copyrighted word processing program having a retail value of $2,600), and also reproduces 10 copies of another computer program copyrighted by a different author and worth more than $2,500, he or she may be charged with two felony counts.

The plain text of the trademark statute demonstrates that it is designed to provide protection for every genuine mark. Likewise, the Copyright Act makes clear that the statute seeks to protect each individual's copyrighted work. See 17 U.S.C.A. § 506. Therefore, charging a defendant with separate counts for violating each of the different copyrights or trademarks can fulfill one of the important purposes of the statute. Further, since reproducing a compilation constitutes multiple violations of the Copyright Act, and since one of the goals of the Act is to protect the individual's copyrighted work, it is proper to charge separate infringing acts against each individual victim as separate offenses. Thus, for example, where multiple copies of separate copyrighted works are contained on a single videocassette tape or CD-ROM disk, the statute would permit multiple charges.

2. Multiple intellectual property crimes committed by the same act

A defendant's acts may criminally violate multiple intellectual property rights. An awareness of the multiple intellectual property crimes that can be charged for the same act can help a prosecutor identify charges more likely to be proven in a particular case or identify additional charges that better capture the breadth of wrongful activities by the defendant.

In cases of copyright infringement arising under 18 U.S.C. § 2319, prosecutors commonly bring counterfeit labeling or trademark counterfeiting charges in addition to, or in lieu of, the pure copyright charge. For example, manufacturers or vendors of infringing items may illegally attempt to reproduce the labels and packaging for genuine copyrighted works. These counterfeit labels will usually support charges under the counterfeit labeling statute, 18 U.S.C. § 2318. The packaging usually carries counterfeit trademarks, which will usually support charges under the trademark counterfeiting statute, 18 U.S.C. § 2320. Indeed, since the offenses of counterfeit labeling and trademark counterfeiting have simpler elements and a lower mens rea than criminal copyright infringement, it may be preferable to charge them and not charge 18 U.S.C. § 2319 at all.

Infringers often reproduce the instruction manuals offered by the legitimate manufacturer, in addition to distributing the infringing goods or works. These instruction manuals are costly to design and produce and many leading manufacturers have a practice of copyrighting them as well. If the instruction manual is copyrighted, reproducing its text can give rise to an another charge of copyright infringement, as well as an additional charge under 18 U.S.C. § 2320 if the infringing copy bears a registered trademark. While the value of the infringed manual may be small compared to the value of the counterfeit items, a separate charge can make clear the defendant's wholesale disregard for, and infringement of, the victim's intellectual property rights.

Sometimes, the act of copying digitized intellectual property may automatically give rise to two separate intellectual property crimes. One important example is with copies of music performances. The infringement of a sound recording generally involves not one, but two separate acts of copyright infringement upon two different copyrighted works. The first infringement is for the musical work, i.e., the notes and lyrics. The other infringement is for the separately copyrighted public performance of the work. Each type of infringement may be charged in a separate count.

A similar dual intellectual property crime may arise with respect to computer software, since computer software often employs a trademarked name, icon, or graphics. For example, a defendant who posts a pirated copy of computer software on an Internet bulletin board under a trademarked name may have committed trademark counterfeiting in addition to copyright infringement. In one litigated civil case, the court granted plaintiff's motion for summary judgment where the defendant operated a bulletin board that facilitated the distribution of plaintiff's computer games via the Internet. When the downloaded game was played, the game began with a screen showing plaintiff's federally registered trademark. The court rejected

defendant's claim that plaintiff's trademark was being used merely "as a file identifier" and that such use does not violate the Lanham Act. The court stated that the use of plaintiff's trademark "creates a likelihood of consumer confusion as to whether Sega endorsed or sponsored the games appearing on or downloaded from MAPHIA [defendant's BBS]." Sega Enters. Ltd. v. MAPHIA, 948 F. Supp. 923, 939 (N.D. Cal. 1996). The court concluded that the defendant's "use of Sega's trademark on virtually identical Sega game programs constitutes counterfeiting." Id. The same logic could be applied under the criminal law.

Charging both copyright and trademark violations arising from the same act or acts does not violate the Double Jeopardy Clause of the Fifth Amendment of the Constitution since "each offense contains an element not contained in the other." United States v. Dixon, 509 U.S. 688, 696 (1993) (citing Blockburger v. United States, 284 U.S. 299, 304 (1932)). Accordingly, inconsistent verdicts from a trial involving charges of copyright infringement and trademark counterfeiting should not jeopardize a successful conviction. See United States v. Sheng, 26 F.3d 135, 1994 WL 198626 (9th Cir. 1994) (unpublished op.) (rejecting claim of inconsistent verdicts where defendant was acquitted on the criminal copyright infringement count and convicted for trafficking in counterfeit goods).

D. The Victim's Role in an Intellectual Property Case

Congress has passed numerous statutes guaranteeing victims' rights during the investigation, prosecution and sentencing stages of all criminal prosecutions. See, e.g., 18 U.S.C. § 1512 (tampering with a witness, victim or an informant). In compliance with these statutes and Department of Justice guidelines, prosecutors must always be mindful of the rights of victims, including but not limited to notification about services and case events, active consultation with government attorneys, the return of property and restitution, and protecting victims' right to privacy without infringing on the constitutional rights of defendants. See generally Attorney General Guidelines for Victim and Witness Assistance (January 31, 2000); United States Attorney's Manual § 3-7.300 to 3-7.340; Markus Dubber, The Victim in American Penal Law: A Systematic Overview, 3 Buff. Crim. L. Rev. 3 (1999).

Victims of intellectual property crimes are entitled to no less consideration. Indeed, as with other white-collar crimes, victims often are intimately involved in the investigation and prosecution of intellectual property crimes:

> It is in the public interest that victims and others expend their time, efforts, and resources to aid public prosecutors. Many so-called white collar crimes are complicated transactions. Knowledgeable people are needed to detect and explain them. It would not serve the public interest to have a rule that inhibited close cooperation between prosecutors and victims.

Commonwealth v. Ellis, 708 N.E.2d 644, 651 (Mass. 1999) (holding statutorily prescribed funding scheme under which insurance companies underwrote the costs of investigations and

prosecutions conducted by state insurance fraud bureau to be permissible). Frequently, corporate victims in intellectual property cases independently investigate suspected infringers, and provide this information to prosecutors. See International Bus. Machs. Corp. v. Brown, 857 F. Supp. 1384, 1389 (C.D. Cal. 1994) (rejecting defendant's allegation that IBM's cooperation with law enforcement was improper and observing that "this court sees no reason why those victims who have the resources and willingness to pursue their own investigation and enforce their own rights should be precluded either from doing so or from sharing the fruits of their efforts with law enforcement agencies").

Such cooperation is not only desirable but often of critical importance. Indeed, in many intellectual property cases, the victim rights holder is a necessary witness to testify with regard to the legitimate, infringed upon item. For example, an author might be needed to authenticate a copyrighted work as his or her creation.

Moreover, recognizing the complex issues of sentencing in copyright and trademark cases, Congress has made special provisions to invite the involvement of victimized rights holders. In any case, 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(b)(4)(D). Those injured by copyright infringement or trademark infringement, including producers and sellers of legitimate works, intellectual property holders, and their legal representatives, are guaranteed by statute 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(d), 2319A(d), 2320(d). Like Congress, prosecutors should recognize the benefits of inviting victims to participate in intellectual property cases.

Prosecutors should, however, be mindful of the risks of such intimate association. In every case, government attorneys must make independent, discretionary decisions during all stages of a criminal case and should exercise care that victim involvement does not complicate the case or, in extreme situations, jeopardize the prosecution itself. Obviously, a prosecutor with personal private interests in the case may run afoul of ethics laws and regulations. See, e.g., 18 U.S.C. § 208 (forbidding participation in a matter in which government officer or employee has a financial interest).

In intellectual property investigations and prosecutions, government attorneys should be cognizant of possible undue victim involvement and its ramifications. Such involvement could create an appearance of impropriety for the law enforcement institution as well as for the individual cases. One case of undue victim involvement in an intellectual property case resulted in a dismissal of charges against the defendant. In California v. Eubanks, 927 P.2d 310 (Cal. 1997), the California Supreme Court concluded that arrangements linking the prosecutor to a private party who had a personal interest in the outcome of the case created an actual conflict of interest and found no abuse of discretion in the trial court's dismissal of all charges against the defendants. Id. at 323. In that case, a corporation had contributed approximately $13,000 toward the costs of a district attorney's investigation of individuals suspected of stealing trade secrets.

The California Supreme Court discussed at length the importance of the independence and impartiality of the local prosecuting authority at all stages of the criminal prosecution:

> The importance, to the public as well as to the individuals suspected or accused of crimes, that these discretionary functions be exercised "with the highest degree of integrity and impartiality, and with the appearance thereof" cannot be easily overstated. . . . The nature of the impartiality required of the public prosecutor follows from the prosecutor's role as representative of the People as a body, rather than as individuals.

Id. at 315 (citation omitted). Although private financing of intellectual property cases is unlikely in federal cases, excessive reliance on information provided by industry investigators may raise similar concerns and in some situations limit the ability of the prosecutor to objectively evaluate the strengths and weaknesses of a case. Naturally, close victim consultation is essential when information or expertise is uniquely in the possession of the victim. For example, law enforcement appropriately may involve the victim of an IP crime to distinguish legitimate goods from counterfeits or to identify proprietary information. However, to minimize any appearance of impropriety, prosecutors should be wary of accepting offers of in-kind assistance of goods or services that could easily be obtained elsewhere, such as provision of simple storage facilities. While there is greater concern when the victim offers such assistance, offers from third parties must also be evaluated carefully and be consistent with the Department policies of acceptance of gifts.

The Department of Justice has established general policy regarding gifts to the Department. Department of Justice order 2400.2 (September 2, 1997). This policy provides that the authority to accept gifts including gifts of services on behalf of the Department or its components has been delegated exclusively to the Assistant Attorney General for Administration and that solicitation of gifts must be approved in advance by the Attorney General or by the Deputy Attorney General. For additional information, contact the Facilities and Administrative Services Staff of the Justice Management Division at (202) 616-2995.

The perceived taint before a court or a finder of fact, that a private party controls the prosecution can have ramifications throughout a criminal proceeding, not just for a decision on a motion to dismiss. It may affect the jury's willingness to assign guilt and the court's sentencing. Courts and the finders of fact can recognize when victims of intellectual property crimes may have a significant financial interest at stake in the prosecution. For example, victims may seek civil redress soon after the conclusion of the criminal case and use the criminal conviction as res judicata. While there is nothing untoward about the civil case succeeding the criminal case, a prosecutor should be aware, when meeting with victims and when evaluating all aspects of a case, of the potential for perceived impropriety. Sharing evidence and close consultation can be appropriate, but steps should be taken to avoid giving the defense any avenue at trial to suggest that the case against the defendant was motivated by the desires of the victim alone. Ultimate decisions concerning investigation strategy, evidence gathering, charging, plea negotiations, trial tactics and sentencing recommendations should all remain as free of this taint as possible. Just as

it would be ill-advised to have the victim of a street crime present when such critical decisions are made, so too should victims of copyright or trademark cases be excluded from such discussions where possible.

VII. CONSEQUENCES OF CONVICTION FOR INTELLECTUAL PROPERTY INFRINGEMENT CRIMES

This chapter discusses the consequences of intellectual property crime. The various copyright and trademark crimes have assorted maximum penalties provided by statute.

Statutory maximum penalties are as follows: A defendant convicted of counterfeit labeling, 18 U.S.C. § 2318; financially motivated copyright infringement of sufficient scale, 18 U.S.C. § 2319; or trafficking in recordings of live musical performances, 18 U.S.C. § 2319A, faces a maximum imprisonment of up to five years. A defendant convicted of trademark counterfeiting, 18 U.S.C. § 2320, faces up to ten years in prison. Generally, the maximum fine for a felony for an individual is $250,000 and for an organization is $500,000, except that in infringement cases, where the offense results in pecurinary gain or loss, a court may award up to the greater of twice the gross gain or the gross loss. 18 U.S.C. § 3571. For trademark counterfeiting, however, the maximum fine is increased to $2,000,000 for an individual or $5,000,000 for an organization. 18 U.S.C. § 2320(a).

Other rules lay out the practical consequences of a conviction. Usually the prison sentence and the fine imposed are determined primarily by application of by the Sentencing Guidelines. Restitution is another important consequence of a conviction. In addition, forfeiture can be an attractive option in cases involving defendants with significant assets. The consequences of a conviction for copyright and trademark crimes are discussed below.

One interesting feature of sentencing for infringement crimes is that 18 U.S.C. §§ 2319(d), 2319A(d) and 2320(d) specifically permit the victims of copyright or trademark infringement, including producers and sellers of legitimate works and holders of intellectual property rights in the infringed work, to submit victim impact statements at sentencing. These statements may describe the extent of the injury and loss suffered, including estimated economic impact resulting from the infringement. They clearly identify the intellectual property right holder as a victim of crime and they can provide a means to supplement the usual requirement that the pre-sentence report contain verified information containing an assessment of the impact on any individual against whom an offense has been committed. Fed. R. Crim. P. 32(b)(4)(D). Of course, economic impact arguments may be weakened or even backfire if the victim is unable to show persuasive evidence that the infringing product actually affected sales or marketing. See, e.g., Twentieth Century Fox Film Corp. v. Suarez Corp. Indus., No. 98 Civ. 1711 (WK), 1998 WL 126065 (S.D.N.Y. Mar. 19, 1998) (holding that the defendant's sales of a movie-related infringing necklace for $19, stemming from advertisements arranged prior to suit which could not be canceled, did not damage the movie maker's reputation or affect ticket sales of the movie "Titanic," the movie company's licensing of a copyrighted $195 necklace, or the movie company's plan to auction a $3.5 million version of necklace for charity and observing that "[w]e cannot believe that any person intent on going to Tiffany's to buy a $200 necklace for a loved one would be deterred by the knowledge that a person of lesser means could go to Woolworth's . . . and get a cheaper one").

A. Sentencing Guidelines

Sentencing for violations of 17 U.S.C. § 506(a), and 18 U.S.C. §§ 2319, 2319A & 2320 is generally governed under the Sentencing Guidelines by § 2B5.3. See United States Sentencing Commission, Guidelines Manual § 2B5.3 (Nov. 1998 & Supp. May 2000) (hereinafter U.S.S.G.). In 1997, Congress directed the Sentencing Commission 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." See No Electronic Theft (NET) Act of 1997, Pub. L. No. 105-147, § 2(g), Dec. 16, 1997. As a result, the Sentencing Commission on May 1, 2000, issued an amended version of U.S.S.G. § 2B5.3. This revised guideline section is discussed here in detail. The previous guideline is discussed below, at Section VII.A.7 at page 112.

The amended guideline became effective on May 1, 2000. Among other changes, the new Guideline increases the base offense level from 6 to 8. U.S.S.G. § 2B5.3(a). It also, in many cases, provides for stiffer penalties by specifically providing for the use of the retail value of the infringed (legitimate) item, instead of the retail value of the infringed-upon (counterfeit or pirated) item, to calculate loss. The specific offense characteristics are set out in Guidelines § 2B5.3(b) as follows:

(1) If the infringement amount exceeded $2,000, increase by the number of levels from the table in § 2F1.1 (Fraud and Deceit) corresponding to that amount.

(2) If the offense involved the manufacture, importation, or uploading of infringing items, increase by 2 levels. If the resulting offense level is less than level 12, increase to level 12.

(3) If the offense was not committed for commercial advantage or private financial gain, decrease by 2 levels, but not less than level 8.

(4) If the offense involved (A) the conscious or reckless risk of serious bodily injury; or (B) possession of a dangerous weapon (including a firearm) in connection with the offense, increase by 2 levels. If the resulting offense level is less than level 13, increase to level 13.

1. Applying the "infringement amount" against the table in § 2F1.1

The first specific offense characteristic provides that if the "infringement amount" exceeds $2,000, the sentencing court is to increase the offense level by the number of levels prescribed in the table in section 2F1.1 for the corresponding amount. U.S.S.G. § 2B5.3(b)(1). Application note 2 explains how to determine the "infringement amount." If a court finds any of 5 circumstances present, it is to calculate the "infringement amount" as the retail value of the

infringed (legitimate) item multiplied by the number of infringing items. U.S.S.G. § 2B5.3 applic. n.2(A). If none of these circumstances apply, the court should calculate "infringement amount" as the retail value of the infringing (counterfeit or pirated) item multiplied by the number of infringing items. U.S.S.G. § 2B5.3 applic. n.2(B). (If the circumstances apply to only some of the infringing items, the court may combine partial calculations. U.S.S.G. § 2B5.3 applic. n.2(D)). This distinction is significant because the true value of the infringed item is usually substantially less than the value of the infringing item although in many cases it can be shown that the retail value of the infringing item can approximate the retail value of the infringed item. Either way, the "retail value" is defined for these purposes as "the retail price of that item in the market in which it is sold." U.S.S.G. § 2B5.3 applic. n.2(C).

a. The five circumstances where the "infringement amount" is based upon the retail value of the infringed (legitimate) item

As noted above, the Guidelines provide five circumstances where the "infringement amount" is based upon the retail value of the infringed (legitimate) item. In those cases, the retail value itself will generally be straightforward to establish by presenting evidence of the regular retail price of the item through legitimate, mainstream outlets.

The following are the five circumstances where the retail value of the infringed (legitimate) item multiplied by the number of infringing items is to be used:

(i) The infringing item (I) is, or appears to a reasonably informed purchaser to be, identical or substantially equivalent to the infringed item; or (II) is a digital or electronic reproduction of the infringed item.

(ii) The retail price of the infringing item is not less than 75% of the retail price of the infringed item.

(iii) The retail value of the infringing item is difficult or impossible to determine without unduly complicating or prolonging the sentencing proceeding.

(iv) The offense involves the illegal interception of a satellite cable transmission in violation of 18 U.S.C. § 2511.

(v) The retail value of the infringed item provides a more accurate assessment of the pecuniary harm to the copyright or trademark holder owner than does the retail value of the infringing item.

Note that in the first subcategory of the first of the five circumstances, the test for non-digital and non-electronic reproductions is whether the infringing item appears to "a reasonably informed purchaser" to be close to an equivalent to the infringed item. U.S.S.G. § 2B5.3 applic. n.2(A)(i)(I). The class of those who are "reasonably informed purchasers" may be a smaller

class, comprising purchasers with more knowledge than "reasonable persons." However, if the infringing item is a digital or electronic reproduction of the infringed item (or if any one or more of the other factors apply) then the sentence is increased by reference to the value of the infringed item, regardless of how the infringing item appears to a reasonably informed purchaser.

In a case involving illegal interception of a satellite cable transmission in violation of 18 U.S.C. § 2511, the "retail value of the infringed item" is the price the user of the transmission would have to paid to lawfully receive that transmission, and the "infringed item" is the satellite transmission rather than the intercepting device. U.S.S.G. § 2B5.3 applic. n.2(A)(i)(III).

b. Circumstances where the "infringement amount" is based upon the retail value of the infringing (counterfeit or pirated) item

Where one of the 5 circumstances described above is not applicable, the "infringement amount" will be based upon the retail value of the infringing (counterfeit or pirated) item. As noted above, the "retail value" is defined as "the retail price of that item in the market in which it is sold." U.S.S.G. § 2B5.3 applic. n.2(C). Determining an accurate retail value of an infringing item may prove difficult, as it did under the previous version of the Guidelines section. In such cases, prosecutors may find it helpful to consider case law established under the prior Guidelines section, which had used the "the retail value of the infringing items" standard in all cases. See infra Section VII.A.7 at page 112.

2. Uploading infringing items increases the level by 2

The second specific offense characteristic provides a 2-point enhancement (or an enhancement to level 12 if the offense level would be less than 12) for offenses involving the "manufacture, importation, or uploading of infringing items." U.S.S.G. § 2B5.3(b)(2). The term "uploading" means that the offender made the "infringing item available on the Internet or a similar electronic bulletin board with the intent to enable others to download or otherwise copy, or have access to, the infringing item." U.S.S.G. § 2B5.3 applic. n.1. The application note explains that this provision applies only to uploading with the intent to enable other persons to download or otherwise copy the infringing item. For example, it would apply to an illegal upload to a publicly accessible Internet site, but not to installation of software on the defendant's home computer. U.S.S.G. § 2B5.3 applic. n.3.

In its supplement accompanying the 2000 amendment, the Commission indicated that uploading counterfeit or pirated items can be particularly damaging to the legitimate owners because, by uploading items to the Internet, the offender is placing these items the stream of commerce, thereby enabling others to infringe the intellectual property. For example, the enhancement will apply where the offender uploads pirated copies of video games or musical recordings to a Web site, thereby making the works instantly available for downloading by anyone with an Internet connection. The Commission estimated that the uploading enhancement

would have been applicable in two-thirds of the cases it reviewed as having been sentenced under the guideline.

3. Offense not committed for profit reduces the level by 2

The third specific offense characteristic provides for a 2 level reduction if the offense was not committed for commercial advantage or private financial gain. Nevertheless, this adjustment would not apply to reduce the offense level less than 8. U.S.S.G. § 2B5.3(b)(3).

4. Offense involving risk of serious bodily injury or possession of a dangerous weapon increases the level by 2

The fourth specific offense characteristic provides for a 2 level enhancement or an offense level of 13, which ever is greater, if the offense involved conscious or reckless risk of serious bodily injury or possession of a dangerous weapon. U.S.S.G. § 2B5.3(b)(4). In its supplement accompanying the 2000 amendment, the Commission indicated that this was motivated by testimony indicating that the risk of serious bodily injury may occur in some cases involving counterfeit consumer products. It therefore provided for an enhancement consistent with an identical enhancement in the fraud guideline. See U.S.S.G. § 2F1.1(b)(6).

5. Decrypting or circumventing security measures

The application note provides a reminder that where the offender takes steps to circumvent encryption or other security measures in order to gain initial access to the infringed item, the sentencing court should make an upward adjustment of 2 levels under U.S.S.G. § 3B1.3. U.S.S.G. § 2B5.3 applic. n.4. In its supplement accompanying the 2000 amendment, the Commission observed that persons who use such a special skill to facilitate or commit a crime generally are viewed as more culpable.

6. Upward adjustments for other factors, including substantial harm to reputation or the furtherance of an organized criminal enterprise

The revised guideline also provides that if the offense level determined under the Guidelines "substantially understates the seriousness of the offense," an upward departure may be warranted. U.S.S.G. § 2B5.3 applic. n.5. The Commission provides two examples of factors that the court may take into account when considering an upward departure. The first is if the reputation of the trademark or copyright owner was substantially harmed by the offense in a way that is not accounted for in the monetary calculation. The second is if the offense was in connection with or in furtherance of a national or international organized criminal enterprise, which the Commission had been told in its public comment, sometimes takes place.

7. Guideline for offenses committed before May 1, 2000

The previous version of U.S.S.G. § 2B5.3 of the Sentencing Guidelines is applicable to offenses committed before May 1, 2000. See United States Sentencing Commission, Guidelines Manual § 2B5.3 (Nov. 1998) (hereinafter U.S.S.G. (1998)). This section set the base offense level at 6. It further directed that "[i]f the retail value of the infringing items exceeded $2000," the sentencing court must increase the offense level by the corresponding number of levels from the fraud table in U.S.S.G. § 2F1.1. See U.S.S.G. § 2B5.3(b)(1) (1998). Unlike the revised guideline, the background commentary to the superseded U.S.S.G. § 2B5.3 (1998) specifically stated that "the enhancement is based on the retail value of the infringing items." Thus, in their previous guise the Guidelines anticipated that, in intellectual property cases, the sentencing court would not engage in a generalized determination of the victims' "loss," or even, as an alternative, a determination of the defendant's "gain." Indeed, the background commentary to the superseded version of U.S.S.G. § 2B5.3 (1998) itself anticipated that a traditional computation of "loss" is not the designated measurement, stating that the value of the infringing items "will generally exceed the loss or gain due to the offense." Moreover, courts uniformly rejected the argument that, once the retail value exceeded $2000, the offense level increase should have been based on the "loss" amount since the term "loss," and not the term "retail value," is used in U.S.S.G. § 2F1.1 to calculate the increase. Rather, courts relied on the clearly stated intent of the background commentary to the superseded version of U.S.S.G. § 2B5.3 (1998) that the enhancement itself is based on the retail value of the counterfeit items, and the fact that U.S.S.G. § 1B1.5 expressly instructs that when one guideline cross-references a particular table in another offense guideline, then only that table is referenced. See United States v. Cho, 136 F.3d 982, 983-84 (5th Cir. 1998) (affirming district court's sentencing calculation concerning defendant's guilty plea for trafficking in counterfeit handbags); cf. United States v. Bao, 189 F.3d 860, 866-67 (9th Cir. 1999) (affirming defendant's conviction for conspiracy to traffic in, and trafficking in, counterfeit computer documentation while vacating sentence and remanding for resentencing).

The Sentencing Guidelines are clear that the reference in U.S.S.G. § 2B5.3 (1998) to the table contained in U.S.S.G. § 2F1.1 applies only to the actual table and not to the entire offense guideline. As U.S.S.G. § 1B1.5(b)(2) provides, "[a]n instruction to use a particular subsection or table from another offense guideline refers to the particular subsection or table referenced, and not to the entire offense guideline." U.S.S.G. § 1B1.5(b)(2). Therefore, it would not be appropriate to apply additional enhancements based upon the commentary to U.S.S.G. § 2F1.1, notwithstanding the fact that several would seem to arise often in the context of intellectual property violations. See, e.g., U.S.S.G. § 2F1.1(b)(2)(A) (discussing cases where defendant's role involved more than minimal planning); U.S.S.G. § 2F1.1(b)(4)(B) (discussing cases where defendant's offense involved a violation of an existing judicial or administrative order).

The "retail value of the infringing items" yardstick is often difficult to measure in practice. Measuring the retail value of legitimate items distributed through conventional retail channels is relatively easy – the retail value generally is measured by what buyers in the legitimate market place are willing to pay for the item, i.e., the price. With respect to counterfeit items, however, the retail value was not always obvious. For example, suppose a counterfeiter

pirates movie videotapes that are essentially indistinguishable in quality and appearance from legitimate tapes. The counterfeiter then sells the bootlegs through two channels. First, he approaches a small video store, represents himself as a legitimate movie distributor, and sells the bootlegs for the same price the store owner would have paid for the videos in the legitimate market place. The counterfeiter also sells copies of the same bootlegged movies on the street for half that price. What is the retail value of the counterfeit items in such a scenario? Should the value of the infringing items be measured by their price to unsuspecting purchasers in the legitimate market place, or their price on the black market, or both?

Finally, with the growth of the Internet, unauthorized copies of software and music are commonly available free-of-charge over the Internet. In such circumstances, it makes little sense to calculate the retail value of the infringing item based on its price – $0 – on the black market. In short, prior to May 1, 2000, the Guidelines did not provide any guidance to courts on how to calculate the "retail value of the infringing items" in the many and varied situations where there was no obvious way to determine a meaningful retail value for the infringing items.

In 1991, the Second Circuit decided United States v. Larracuente, 952 F.2d 672 (2d Cir. 1991), the leading case on assessing the retail value of infringing goods where they are sufficiently similar in quality to the genuine items sold to innocent customers through legitimate retail channels. In Larracuente, the defendant, the owner and operator of a videotape rental store, was convicted of criminal copyright infringement for the unauthorized reproduction of movie videotapes. During the trial, a witness for the defense testified that bootleg tapes generally sold for between $10 and $15 on the black market. However, in calculating the total "retail value of the infringing items" for sentencing purposes, the trial court applied the retail price of the legitimate tapes, which was $73, in part because the tapes were of sufficient quality to permit their distribution in the legitimate market. Id. at 674. On appeal, the Second Circuit held that the sentencing court was correct in basing its guideline calculations on the normal retail price, as opposed to the lower bootleg price that would be "paid by those who presumably are aware that the copies they are buying are not legitimate." Id. at 674. The court reasoned that "[w]here, as here, unauthorized copies are prepared with sufficient quality to permit their distribution through normal retail outlets, the value of the infringing items is their normal retail price to ultimate consumers who purchase from such outlets." Id. The court also noted in dicta, however, that it would be facing a different question if the infringing items were "of obviously inferior quality" and were "for that reason distributed to consumers who pay far less than the retail price for authentic items." Larracuente, 952 F.2d at 675.

A number of other courts similarly recognized the relevance of the price of the genuine item when determining the retail value of the infringing items where that value is otherwise not easily determined. See, e.g., United States v. Bao, 189 F.3d 860, 866-67 (9th Cir. 1999) (stating that the retail value of the genuine merchandise is relevant and can serve as a ceiling in determining the retail value of the infringing items); United States v. Cho, 136 F.3d 982, 985 (5th Cir. 1998) (citing United States v. Kim, 963 F.2d 65 (5th Cir. 1992) for the proposition that it is not clear error for the district court to rely on the retail value of the genuine items in assessing the

retail value of the counterfeit items, particularly given testimony as to the difficulty of calculating the retail price of counterfeit items); United States v. Kim, 963 F.2d 65, 69 (5th Cir. 1992) (holding that because the defendant offered no evidence regarding the retail value of the counterfeit items, the evidence offered by the government as to the retail value of the genuine merchandise was relevant for setting a retail value for the counterfeit items)[12]; United States v. DeFreitas, No. 98 CR. 1004 (RWS), 2000 WL 763850, at *2 (S.D.N.Y. June 13, 2000) (citing United States v. Bao with approval). Indeed, in Bao, Kim, and DeFreitas, the courts relied ultimately on the legitimate retail price of the infringed good, or a comparable item sold through normal retail channels, when determining the appropriate sentencing enhancement under the guidelines, notwithstanding their express recognition that, pursuant to the plain language of the guideline, the phrase "retail value of the infringing items" refers to the retail value of the counterfeit merchandise. See Bao, 189 F.3d at 867; Kim, 963 F.2d at 67-68; DeFreitas, 2000 WL 763850, at *2.

B. Restitution

Restitution is an important consequence of intellectual property enforcement and can play a substantial role in making the victim whole. Because intellectual property can be (and usually is) infringed without the knowledge of the victim rights-holder, prosecutors may overlook restitution when planning the disposition of a case. It is not uncommon for intangible property to be recognized as property by the federal courts. See, e.g., United States v. Carpenter, 484 U.S. 19, 26 (1987) (holding confidential information, another type of intangible property, to be protected by mail and wire fraud statutes and stating that it has "long been recognized as property"). Restitution has been awarded for infringement crimes in many cases. See, e.g., 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 for in a case of mail and wire fraud and copyright infringement in connection with 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, 45 F.3d 577, 579 (1st Cir. 1995) (same; amount of $100,000); United States v. Hicks, 46 F.3d 1128, No. 92-5429, 1195 WL 20791, at *3 (4th Cir. Jan. 20, 1995) (unpublished op.) (upholding restitution award in satellite decryption and copyright case); United States v. Trevino, 956 F.2d 276, No. CR-90-0022-CBM-1, 1992 WL 39028, at *2 (9th Cir. Feb. 28, 1992) (upholding restitution award of $1,233,830 as the cost of replacement power for nuclear generating station shut down upon discovery that circuit breakers were counterfeit). In fact, since infringement crimes are

---

[12] The court in Kim analyzed the previous U.S.S.G. § 2B5.4 (Criminal Infringement of Trademark) and not U.S.S.G. § 2B5.3 (1998). Nevertheless, after Kim was decided, the previous § 2B5.4 was deleted in its entirety and consolidated with § 2B5.3. See U.S. Sentencing Guidelines Manual, Appendix C, Amendments 481 and 482 (effective November 1, 1993). Since the language in the former U.S.S.G. § 2B5.4 was identical to the present § 2B5.3 and was consolidated into U.S.S.G. § 2B5.3 (1998), Kim remains good authority for that provision.

offenses "against property," and because identifiable victims, such as the victim rights-holders, have suffered a "pecuniary loss," restitution is mandatory under federal law. See 18 U.S.C. § 3663A(c)(1)(A)(ii); United States Sentencing Guidelines Manual § 5E1.1. Where, as in intellectual property cases, infringement crimes are committed for financial gain, defendants often have an ability to pay substantial restitution promptly.

Because infringement is at the heart of every intellectual property crime, the holder of the copyright or trademark is a victim – an entity directly and proximately harmed. See 18 U.S.C. § 3663A(a)(2) (defining "victim" as a person directly and proximately harmed as a result of a commission of an offense). Prosecutors should also consider all victims that suffered a loss – from the holder of the intellectual property to the direct purchaser and the ultimate consumer of the infringing good – but only those losses arising from the conduct underlying the offense of conviction. See, e.g., United States. v. Cobbs, 967 F.2d 1555 (11th Cir. 1992) (vacating restitution order based on loss arising from use of unauthorized credit cards where conviction was for possession of credit cards). Prosecutors often seek restitution for the victim rights-holder only because other potential victims, such as consumers, may constitute an impracticably large or difficult to identify class, or may raise complex issues of fact that would unduly burden the sentencing process. See 18 U.S.C. § 3663A(c)(3). Where practicable, all identifiable victims should be identified for restitution, even if they are not located. See United States v. Berardini, 112 F.3d 606, 609-12 (2d Cir. 1997) (upholding award of restitution for fraud to identified but unlocated victims).

In contrast to the calculation of loss under the sentencing guidelines, restitution is awarded for actual, not intended loss. "Unlike the Guidelines, which permit the court to consider actual or intended loss for the purposes of determining the sentencing level, 18 U.S.C. § 3663A requires an award of restitution to be based on the amount of loss actually caused by the defendant's offense." United States v. Brierton, 165 F.3d 1133, 1139 (7th Cir. 1999) (vacating restitution order and citing U.S.S.G. § 2F1.1 in bank fraud case). See also United States v. Messner, 107 F.3d 1448, 1455 (10th Cir. 1997) (vacating restitution order and instructing trial court to base the amount of restitution solely on actual losses in bankruptcy fraud case). See, e.g., United States v. Palomba, 182 F.3d 1121, 1122 n.2 (9th Cir. 1999) (noting the difference between restitution and sentencing loss as the difference between actual loss and intended loss in surety fraud case); United States v. Germosen, 139 F.3d 120, 130 (2d Cir. 1998) (contrasting Application Note 7 to § 2F1.1 of Guidelines with 18 U.S.C. § 3663(a)(1)(A) in wire fraud case). But cf. United States v. Manzer, 69 F.3d 222, 230 (8th Cir. 1995) (upholding restitution award of $2.7 million for in a case of mail and wire fraud and copyright infringement because "a conviction for mail or wire fraud can support a conviction for a broad scheme regardless of whether the defendant is convicted for each fraudulent act within that scheme" and looking to "the scope of the indictment to determine whether it details a broad scheme encompassing transactions 'beyond those alleged in the counts of conviction'" (citing cases)).

Federal law permits the court to require the defendant to pay an amount equal to the value of the property damaged, lost, or destroyed, 18 U.S.C. § 3663(b)(1)(B)(i); and to order restitution

to each victim "in the full amount of each victim's losses." 18 U.S.C. § 3664(f)(1)(A). However, it is sometimes not immediately apparent how to fully value the "loss" to the victim rights-holder in an intellectual property case. This difficulty may arise because, in the absence of a legal regime, intellectual property has characteristics of a public good, such as being "non-excludable." See, e.g., William M. Landes & Richard A. Posner, An Economic Analysis of Copyright Law, 18 J. Legal Stud. 325, 326 (1989) ("A distinguishing characteristic of intellectual property is its 'public good' aspect."). Therefore, a defendant might even claim that his infringement of the victim's intellectual property caused no actual "loss" to the victim because even after infringement the victim was still free to use the intellectual property itself. This argument is without merit because it is the right to control the intellectual property (as distinguished from a particular copy of the intellectual property) that the defendant has unilaterally divested from the victim.

Prosecutors may find it especially helpful in intellectual property cases to seek information from the victim. Such consultation would supplement the notice of sentencing that prosecutors should provide to victims. 42 U.S.C. § 10607(c)(3)(G); Attorney General Guidelines for Victim and Witness Assistance Art. IV.B.2.a(1)(e), at 31 (January 31, 2000). As noted above, victims of intellectual property crimes have a formal means of providing victim impact statements as provided by 18 U.S.C. §§ 2319(d), 2319A(d), 2320(d) as a supplement to the provisions of the pre-sentence report that includes a verified assessment of victim impact in every case. Fed. R. Crim. P. 32(b)(4)(D). Relevant trade associations can also provide helpful guidance. For a list of trade association contacts, see Appendix A.

With a dearth of case law addressing restitution calculations in intellectual property cases, the Computer Crime and Intellectual Property Section provides a variety of theories below that may be useful computing "loss" for restitution purposes in particular cases. In their efforts to calculate the victims' "loss" in intellectual property cases, prosecutors should ensure that the calculation of "loss" is not too complex. See 18 U.S.C. § 3663A(c)(3)(B). Prosecutors should also be careful to distinguish valid losses from consequential damages which may not be covered by the restitution provisions. Compare United States v. Trevino, 956 F.2d 276, No. CR-90-0022-CBM-1, 1992 WL 39028, at *2 (9th Cir. Feb. 28, 1992) (upholding restitution award of $1,233,830 as the cost of replacement power and not "revenue loss") with United States v. Mikolajczyk, 137 F.3d 237, 245-46 (5th Cir. 1998) (distinguishing valid restitution of attorney's fees for defendant's frivolous lawsuits as a direct and mandatory result of the defendant's offense from attorney's fees in a voluntary action to recover property or damages), cert. denied, 119 S. Ct. 250 (1998).

Inventory measure. Restitution may be awarded based on infringing items in the defendant's possession at the time of the investigation, as well as infringing items previously sold or distributed. The amount of infringing items actually in the defendant's possession is often much smaller than the amount that had previously been distributed. Nevertheless, substantial inventory-based restitution may be awarded. For example, the "loss" to the victim could be that the defendant manufactured or purchased an infringing item rather obtaining a legitimate item.

Additionally, if the government can show that the defendant had a regular practice of selling infringing products, but has limited evidence available on the size of the past sales, it could base a restitution analysis on the defendant's inventory.

Key factors. In establishing a formula for restitution in intellectual property cases, there are three significant factors to consider: (1) the quality of the infringing items; (2) the price at which they were sold, and (3) how the items were distributed. In many cases, the first two factors are sufficient to establish a loss figure.

High-quality infringement at market prices. For example, if the defendant sells infringing items of a quality indistinguishable from the legitimate items and at about the same price (the retail price if the defendant is a retailer; the wholesale price if the defendant is a wholesaler), then a reasonable inference may be made that the defendant's sales represent "lost sales" to the victim. A reasonable estimate of the amount of money the victim would have received from those "lost sales" can be computed from the number of infringing items multiplied by the victim's loss per item. The victim's loss per item may be measured, as appropriate for the case, by the wholesale price, the retail price, or the profit per item. For example, in cases involving large inventories of pirated motion pictures, courts may use the wholesale price of the infringed-upon movie. Or in cases of unauthorized decryption of premium channel satellite broadcasts, courts may credit analytical estimates of revenue loss by victims based on revenue records and client lists. See United States v. Manzer, 69 F.3d 222, 229-30 (8th Cir. 1995) (upholding restitution award in descrambler case of $2.7 million as "conservative" where HBO provided analytical loss figure of over $6.8 million). See also United States v. Hicks, 46 F.3d 1128, No. 92-5429, 1195 WL 20791, at *1 (4th Cir. Jan. 20, 1995) (unpublished op.) (capping total amount of fine and restitution to total cost of one-year subscription to infringed premium cable channels).

Proxy valuations may be helpful as well. For example, because the defendant usually sells the infringing items at no more than the price charged by the victim, the defendant's gain may sometimes be used as a simple alternative way to calculate a figure no greater than the victim's loss. United States v. Hicks, 46 F.3d 1128, No. 92-5429, 1195 WL 20791, at *2 (4th Cir. Jan. 20, 1995) (unpublished op.) (upholding restitution award based on defendant's fee to modify cable descrambling devices where not presented with information to establish with certainty the lost revenue for the service providers represented by unauthorized access to 15 channels). And, in conjunction other evidence, a court might find it useful to consider statutory damages that would be awarded in a civil case. 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 provided for violations of a variety of intellectual property rights. See 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).

Low-quality infringement at market prices. If the defendant sells infringing items of a substantially lower quality than legitimate items at about the same price (the retail price if the defendant is a retailer; the wholesale price if the defendant is a wholesaler), then a reasonable inference may be made that the defendant's sales represent "lost sales" to the victim rights holder and a fraud on the victim consumers, both of which are harms anticipated by the intellectual property laws. The defendant may be liable for both of these harms. The "lost sales" value can be measured by the calculation described above. If the victim consumers can be identified, the court may also order that restitution be paid to them in the amount of the purchase price.

High-quality infringement at low prices. In some cases, the infringing items are of a quality indistinguishable from the legitimate items and are sold at a significant discount. In such cases, a third factor is worth considering: how the infringing items were distributed. For example, if the defendant sold the items in quantities to resellers who foreseeably would resell them at about the same price as legitimate items, the resellers effectively "launder" the items. In this context, the result of the defendant's wrongful conduct would be "lost sales" for the victim. Therefore, the victim's "loss" for restitution purposes should also be measured by the number of infringing items multiplied by the victim's loss per item.

Perfect infringement for free. The most extreme example of high-quality intellectual property infringed at a steep discount involves copyrighted digital works, such as music or movies, available for free download via the Internet. In these cases, the infringing work is of identical quality to the infringed-upon item, and is provided directly to the end-user. The availability of free perfect copies of a particular work can undermine the victim's ability to maintain commercial operations. However, if the consumers paid a low price, if any, to the defendant, it may be difficult to argue that all of the copies represent possible lost sales to the victim. Nevertheless, the harm caused by the defendant may be so manifest by the circumstances of the case so as to permit the court to credit the victim with substantial lost revenue. See United States v. Manzer, 69 F.3d 222, 229-31 (8th Cir. 1995) (upholding restitution of $2.7 million for sale of 270 modification and cloning packages for unauthorized decryption of premium channel satellite broadcasts). Moreover, prosecutors may introduce additional evidence concerning the effect that the availability of the high-quality infringing works had on the market for the victim's product. This measure has been upheld in civil copyright infringement cases. See Brooktree Corp. v. Advanced Micro Devices, Inc., 977 F.2d 1555, 1579 (Fed. Cir. 1992) (upholding "actual damages" calculation based upon evidence that plaintiff had been forced to lower its prices as a result of defendant's infringing activities).

Low quality infringement at low prices. If the defendant is trafficking in items that are far removed from the infringed item in both quality and price, then a "lost sales" rationale may be difficult for the prosecutor to sustain for purposes of restitution. For example, if the defendant had been selling counterfeit name-brand watches from a suitcase on a city sidewalk for $20,

rather than the $1,000 price of authentic watches in stores, it would be hard to argue that the counterfeit sales represent significant lost opportunities to sell authentic watches to those purchasers. Identifying the victim's losses in such cases may require a more elaborate factual foundation. For example, the prosecution could provide expert testimony regarding the value of the intellectual property at issue, such as the trademark, and whether that value has been reduced by the defendant's piracy or counterfeiting activities.

C. Forfeiture

The general civil forfeiture provisions are found in 18 U.S.C. § 981. As a result of the recent amendment to 18 U.S.C. § 981(a)(1)(C) by the Civil Asset Forfeiture Reform Act of 2000 ("CAFRA"), any property may be forfeited that is proceeds of a violation of a variety of offenses, including any offense specified as unlawful activity under the money laundering provisions. This list, set out at 18 U.S.C. § 1956(c)(7), includes the following intellectual property crimes: copyright infringement, 18 U.S.C. § 2319; and trademark counterfeiting, 18 U.S.C. § 2320.

The general criminal forfeiture provisions are found in 18 U.S.C. § 982. Another result of CAFRA is that it created general criminal forfeiture authority where general civil forfeiture authority exists. "If a forfeiture of property is authorized in connection with a violation of an Act of Congress, and any person is charged in an indictment or information with such violation but no specific statutory provision is made for criminal forfeiture upon conviction, the Government may include the forfeiture in the indictment or information in accordance with" appropriate procedures. 28 U.S.C. § 2461(c). Taken together with the civil forfeiture provisions described above, this section authorizes criminal forfeiture of proceeds of violations of 18 U.S.C. §§ 2319-2320.

In intellectual property cases, prosecutors often also have the option of invoking specialized civil and criminal forfeiture provisions that relate to the infringing items or the equipment used to create them. The nuances of these provisions are discussed below.

In light of the special procedures and practices in the forfeiture area, prosecutors with questions should contact the forfeiture expert in their office or the Criminal Division's Asset Forfeiture and Money Laundering Section at (202) 514-1263.

1. Civil forfeiture provisions specific to intellectual property cases

Title 17 provides for civil forfeiture remedies in cases of copyright infringement. The government may institute a civil forfeiture action under 17 U.S.C. § 509(a) against the property that has been manufactured or used in violation of the copyright laws. This section provides for forfeiture of three classes of property: (1) the infringing copies, or copies intended for infringing use; (2) the plates, masters or other means used for reproducing the infringing copies; and (3) the devices for manufacturing, reproducing, or assembling the infringing copies. See 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 19 U.S.C. and the provisions relating to in rem Admiralty actions). Other civil forfeiture authority is provided in 18 U.S.C. § 2318(e) for cases of counterfeit labeling.

Civil forfeiture is specifically available for many infringing imported items, depending upon the circumstances. For example, the Customs Service may seize, forfeit, and destroy imported copyright-infringing products administratively under 17 U.S.C. § 603(c). Seizure and forfeiture is also authorized for imported works that violate the law against unauthorized trafficking in recordings of live musical performances. See 18 U.S.C. § 2319A(c). The Customs Service may also seize, forfeit, and destroy imported trademark-infringing products administratively under 19 U.S.C. § 1526(e).

Aside from the importation context, there is no specialized civil forfeiture authority for trademark cases. There is, however, one trademark provision that resembles a civil forfeiture provision. It provides 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). However, this is not a typical forfeiture provision since, inter alia, it does not give a court the discretion to permit the United States to dispose of the assets as it sees fit. Moreover, it applies only when a criminal case has been brought, i.e., it applies to articles in the defendant's possession "in a prosecution under" 18 U.S.C. § 2320. Therefore, it is doubtful that a civil forfeiture action could be brought against the offending res independent of an ancillary prosecution.

It is helpful for prosecutors to recognize that trademark owners have an ex parte seizure remedy available under the Lanham Act, 15 U.S.C. §§ 1051-1127, for infringing products and manufacturing equipment. Prosecutors should be aware of these civil seizure provisions since they may need to participate in the civil proceedings to preserve evidence that may be relevant to an ongoing or developing criminal case, to contest the issuance of an order, to preserve an ongoing investigation, or to invite the trademark owner to initiate a parallel civil case to take advantage of the ability to seize, forfeit, and destroy equipment used to manufacture the counterfeit trademark goods. Trademark owners may also petition the court for seizure orders in the context of a civil action that is brought against an infringer under 15 U.S.C. § 1114. Authority for such an ex parte seizure order is provided at 15 U.S.C. § 1116(d)(1)(A). The Lanham Act requires that trademark owners seeking such an order give reasonable notice to the United States Attorney for the judicial district in which the order is sought; it specifically notes that 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). It further states that "[t]he court may deny such application if the court determines that the public interest in a potential prosecution so requires." Id. In addition, the statute requires that seizure of the infringing goods be made by a federal, state, or local law enforcement officer. See 15 U.S.C. § 1116(d)(9).

2. Criminal forfeiture provisions specific to intellectual property cases

The availability of such sanctions as criminal forfeiture and destruction of a defendant's copyright-infringing merchandise and related equipment varies depending on the crime charged. Certain criminal forfeiture provisions relate to specific intellectual property violations: counterfeit labeling, copyright infringement, trafficking in recordings of live musical performances, and trademark counterfeiting. Of this group, only one provision – that concerning copyright infringement – provides for forfeiture of the equipment used to commit the crime, in addition to forfeiture of the infringing items themselves.

Criminal forfeiture can be an important consideration when investigating and charging a case, not just after conviction. For example, to ensure fulfilling particularity requirements, a seizure warrant may contain a specific reference to infringing items (whether or not property of a target) as subject to seizure and forfeiture pursuant to the relevant statutory authority. At the time of an indictment, if the defendant has in his possession a significant amount of infringing items or equipment used to commit copyright infringement, prosecutors should consider a forfeiture count in the indictment, as well as a seizure warrant. 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.

18 U.S.C. § 2318, which prohibits trafficking in counterfeit labels, contains a mandatory forfeiture provision. Section 2318(d) requires the court to order, as part of any judgment of conviction, "the forfeiture and destruction or other disposition of all counterfeit labels and all articles to which counterfeit labels have been affixed or which were intended to have had such labels affixed." 18 U.S.C. § 2318. Although this does not incorporate criminal forfeiture procedures from 21 U.S.C. § 853, nonetheless this provision is operative only upon conviction. There is no provision in the statute for equipment used in the offense. In most cases the counterfeit labels should be destroyed as well as those items to which they have been affixed, unless the items can be modified to remove the counterfeit label and any other infringing indicia. One creative option would be to then donate the goods to a charity, presumably modified in such a way so that they will not be resold.

The criminal forfeiture provision for criminal copyright infringement requires a court, upon entering a judgment of conviction, to "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). This provision is slightly broader than the provision for trafficking in counterfeit labels, and includes the equipment used in the offense. If the items can bring some value at auction and are unlikely to further damage the copyright holder, prosecutors should argue that no purpose is served by the court ordered destruction of non-infringing items, such as equipment.

A similar forfeiture provision is available for trafficking in unauthorized recordings of live musical performances. See 18 U.S.C. § 2319A(b). One significant difference is that

forfeiture of equipment used to reproduce infringing copies 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." 18 U.S.C. § 2319A(b).

The trademark statute provides 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). This is not a typical forfeiture provision since, inter alia, it does not grant a court the discretion to allow the United States to alienate these assets to third parties. Though it may seem unusual, Congress deliberately declined to include any conviction requirement under this section. Its rational was that "[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." 130 Cong. Rec. 31, 674 (1984) (joint statement at H12077). See also S. Rep. No. 98-526 at 3627 (1984).

VIII. THEFT OF COMMERCIAL TRADE SECRETS

A. Introduction

Until 1996 there was no federal statute that explicitly criminalized the theft of commercial trade secrets. Cf. 18 U.S.C. § 1905 (providing, inter alia, misdemeanor sanctions for the unauthorized disclosure of government information, including trade secrets, by a government employee). Federal courts, however, under limited circumstances, did uphold convictions for the interstate transportation of stolen trade secrets or proprietary economic information under 18 U.S.C. § 2314, or for the disclosure of information in violation of a confidential or fiduciary relationship under 18 U.S.C. § 1341 or 1343.

Because federal prosecutors sometimes had trouble "shoe-horning" the theft of trade secrets into the above statutes and because of the increased recognition of the increasingly important role that intellectual property plays in the well-being of the American economy, Congress enacted the Economic Espionage Act of 1996, effective October 11, 1996. See Pub. L. No. 104-294, 110 Stat. 3489. In general, it criminalizes the theft of trade secrets.

In considering cases under this new statute, prosecutors may find other resources to be helpful as well, including treatises or law review articles. See, e.g., Roger Milgrim, Milgrim on Trade Secrets (1994); Michael Coblenz, Intellectual Property Crimes, 9 Alb. L.J. Sci. & Tech. 235 (1999); Randy Gidseg et al., Intellectual Property Crimes, 36 Am. Crm. L. Rev. 835 (1999); James H.A. Pooley, Mark A. Lemley, & Peter J. Toren, Understanding the Economic Espionage Act of 1996, 5 Tex. Int. Prop. L.J. 177 (Winter 1997). Forms providing a sample indictment and jury instructions for theft of trade secrets, 18 U.S.C. § 1832, are provided in Appendix E at page 184.

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

1. Overview of the statute

The Economic Espionage Act of 1996 ("EEA") contains two separate provisions that criminalize the theft or misappropriation of trade secrets. The first provision, codified at 18 U.S.C. § 1831(a), is directed towards foreign economic espionage and requires that the theft of the trade secret be done to benefit a foreign government, instrumentality, or agent. It states:

> (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 person 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.

In contrast, the second provision, 18 U.S.C. § 1832, makes criminal the commercial theft of trade secrets, carried out for purely economic or commercial advantage:

(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.

Reflecting the more serious nature of foreign government-sponsored economic espionage, an individual convicted of violating 18 U.S.C. § 1831 can be imprisoned for up to 15 years and fined $500,000 or both, whereas a defendant convicted for theft of trade secrets under 18 U.S.C. § 1832 can be imprisoned for up to 10 years and fined $250,000 or both. See 18 U.S.C. §§ 1831(a)(4), 1832(a)(5). Organizations found guilty under the EEA can be fined can be fined up to $10 million for violating § 1831 or $5 million for violating 18 U.S.C. § 1832.

There are a number of important features to the EEA, including a provision for the criminal forfeiture of any property or proceeds derived from a violation of the statute. See 18 U.S.C. § 1834. The EEA also permits the Attorney General to institute civil enforcement actions and obtain appropriate injunctive relief for violations. See 18 U.S.C. § 1836. Furthermore, because of the recognized difficulty of maintaining the secrecy of a trade secret during litigation, the EEA requires that courts take such actions as necessary to preserve the confidentiality of the trade secret. See 18 U.S.C. § 1835. As discussed in a separate section below, the implementation of this particular provision of the EEA has already caused considerable controversy in the pretrial stages of EEA cases.

The EEA also covers attempts and conspiracies to violate the EEA; conduct occurring outside the United States, where the offender is a citizen or permanent resident alien of the United States; and acts in furtherance of the offense that were committed in the United States. See 18 U.S.C. § 1837. Finally, until October 11, 2001, all prosecutions brought under the EEA must first be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General of the Criminal Division. Pursuant to this requirement, the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice has been designated to coordinate requests for approval for 18 U.S.C. § 1832 cases. The Internal Security Section coordinates requests for approval for 18 U.S.C. § 1831 cases. See infra Section VIII.B.11 at page 147 (discussing Department of Justice oversight).

2. Elements common to 18 U.S.C. §§ 1831, 1832

The EEA contains two separate sections that criminalize the theft of trade secrets. Under either section, to obtain conviction for a completed offense, the government must prove beyond a reasonable doubt that: (1) the defendant stole, or without authorization of the owner, obtained, destroyed or conveyed information; (2) the defendant knew or believed that this information was a trade secret; and (3) the information was in fact a trade secret. In addition to these elements, to establish a violation 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, foreign instrumentality, or foreign agent.

If the government cannot establish that the defendant acted with the intent to benefit a foreign entity, the government can establish a violation of 18 U.S.C. § 1832 if it can establish, 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.

As noted, both sections also explicitly criminalize attempts and conspiracies to take trade secrets. See 18 U.S.C. §§ 1831(a)(4)-(5), 1832(a)(4)-(5). Additionally, both sections criminalize the knowing receipt, purchase, destruction or possession of a stolen trade secret. See 18 U.S.C. §§ 1831(a)(3), 1832(a)(3). An analysis of each of the elements of completed offenses are discussed in detail below. The applicable legal analysis for attempts and conspiracies is set forth in the next section.

a. Misappropriation

The initial element of a criminal prosecution under either § 1831 or § 1832 is that the defendant obtained, destroyed or conveyed information without the authorization of the owner. The type of acts which are prohibited are broadly defined and include traditional instances of theft, i.e., where the object of the crime is physically removed from the owner's possession. See 18 U.S.C. §§ 1831(a)(1), 1832(a)(2). However, less traditional methods of misappropriation and destruction are also included within the terms of the EEA. Under 18 U.S.C. §§ 1831(a)(2), 1832(a)(2), the prohibited acts include copying, duplicating, sketching, drawing, photographing, downloading, uploading, altering, destroying, photocopying, replicating, transmitting, delivering, sending, mailing, communicating, or conveying. With many of these methods the original property may not necessarily leave the custody or control of the owner, but the unauthorized duplication or misappropriation may reduce or destroy the value of the owner's property. It was the intent of Congress "to ensure that the misappropriation of intangible information is prohibited in the same way that the theft of physical items are protected." S. Rep. No. 359, 104th Cong., 2d Sess. 16 (1996).

The crux of the misappropriation element of the statute is that the government must prove that the defendant acted "without authorization" from the owner. According to the legislative history, "authorization is the permission, approval, consent or sanction of the owner" to obtain, destroy or convey the trade secret. 142 Cong. Rec. S12202, S12212 (daily ed. Oct. 2, 1996). Thus, for example, where an employee has authorization from his employer to possess a trade secret during the regular course of employment, he can still violate the EEA if he "conveys" it to a competitor without his employer's permission.

b. Knowledge

The first mens rea element that the government must prove in an EEA case is that the defendant's misappropriation was done "knowingly." Generally, under criminal statutes covering the theft of tangible property, the government must prove that the defendant knew that

the object he stole was property that he had no lawful right to convert for his personal use. Thus, in an EEA context, the government must show generally that the defendant knew or had a firm belief that the information he or she was taking was a trade secret. Obviously, however, whether information constitutes a "trade secret" is a legal determination requiring a consideration of the factors set forth in 18 U.S.C. § 1839(3). Prosecutions under this statute would be nearly impossible if the government were required to show in every case that the defendant had performed a detailed analysis of whether the stolen information constituted a trade secret under the multi-part definition set forth in 18 U.S.C. § 1839. Requiring this level of knowledge on the part of a defendant would be squarely at odds with Congress's observation that the knowledge requirement should not be a significant obstacle to appropriate prosecutions:

> This 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 to ensure that the theft of intangible information is prohibited in the same way that the theft of physical items are protected.

142 Cong. Rec. S12202, S12213 (daily ed. Oct. 2, 1996). Based on this legislative explanation, proving that a defendant was aware of proprietary markings, security measures and confidentiality agreements should be sufficient to establish the knowledge element of the statute. More generally, the knowledge element of this statute is satisfied if the government can prove that the defendant knew or had a firm belief that the information to be taken had the attributes of a trade secret as described in 18 U.S.C. § 1839 — that is, the defendant believed 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. See 142 Cong. Rec. at S12213 (daily ed. Oct. 2, 1996) ("For a person to be prosecuted, the person must know or have a firm belief that the information he or she is taking is proprietary."). It is not necessary that the defendant himself have drawn the conclusion that the information was a trade secret. On the other hand, a person who takes a trade secret because of ignorance, mistake or accident, or who actually believes that the information is not proprietary after taking reasonable steps to warrant such belief, cannot be prosecuted under the EEA

c. Trade secret status

The definition of the term "trade secret" under the EEA is very broad. As defined at 18 U.S.C. § 1839, it includes, generally, all types of information, however stored or maintained, which the owner has taken reasonable measures to keep secret and which 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.

This definition is broader than other definitions of "trade secret," including notably the definition of "trade secret" in the Uniform Trade Secrets Act[13] in a number of respects, but prior case law should be instructive in illuminating the EEA's definition of a trade secret. As the First Circuit recently noted, "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, No. 00-1039, 2000 WL 1376377, at *6 (1st Cir. Sept. 28, 2000) (affirming conviction for conspiracy to steal trade secrets).

Novelty. Unlike patents, which must be both novel and a step beyond "prior art," trade secrets must be only "minimally novel." See Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974) (reinstating permanent injunction under Ohio trade secret law against rival chemical company); Buffets, Inc. v. Klinke, 73 F.3d 965, 968 (9th Cir. 1996) (affirming inapplicability of trade secret statute in case involving restaurant chain's recipes and manuals); Arco Indus. Corp. v. Chemcast Corp., 633 F.2d 435, 442 (6th Cir. 1980) (holding that certain method of manufacturing grommets was not protectable under Michigan trade secret law).

In other words, a trade secret must contain some element that is not known and sets it apart from what is generally known. According to the legislative history of the EEA, "[w]hile we do not strictly impose a novelty or inventiveness requirement in order for material to be

---

[13] Section 1(4) of the Uniform Trade Secrets Act provides:

> (4) "Trade secret" means information, including a formula pattern, compilation, program, device, method technique, or process that
>
> (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
>
> (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

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. S12201, S12212 (daily ed. Oct. 2, 1996).

Secrecy. The key attribute of information constituting a trade secret under 18 U.S.C. § 1839 is that it is not generally known to, or reasonably ascertainable by proper means by, the public. Whether the information was secret before it was obtained by the defendant is a question of fact. The government often has the difficult burden of proving a negative, i.e., that the information was not generally available to the public. In this regard, prosecutors should make sure that the information has not been publicly disclosed through, for example, technical journals or other publications. In addition, the prosecutor should determine whether the information was obvious to the victim's competitors in the industry. Sometimes information that a company regards as its proprietary "crown jewels" is well-known in the industry and, therefore, not protected. On the other hand, if a trained scientist is able to glean information from publications that would lead him to deduce a particular formula only after many hours of laboratory testing and analysis, the publication of such articles would not necessarily vitiate trade secret protection, since the scientist's work would not qualify as "reasonably ascertainable by the public."

Furthermore, every part of the information need not be completely confidential to qualify for protection as a trade secret. A trade secret can include a combination of elements that are in the public domain, if the trade secret constituted a unique, "effective, successful and valuable integration of the public domain elements." Buffets, Inc. v. Klinke, 73 F.3d 965, 968 (9th Cir. 1996) (affirming inapplicability of trade secret statute in case involving restaurant chain's recipes and manuals); Metallurgical Indus., Inc. v. Fourtek, Inc., 790 F.2d 1195, 1202 (5th Cir. 1986) (concerning trade secrets involving zinc recovery furnaces and tungsten reclamation process); Rivendell Forest Prods. Ltd. v. Georgia-Pacific Corp., 28 F.3d 1042, 1046 (10th Cir. 1994) (concerning lumber industry trade secrets); see also Lawfinders Assoc., Inc. v. Legal Research Ctr., Inc., 65 F. Supp.2d 414, 423 (N.D. Texas 1999) (concerning legal research trade secrets); Apollo Techs. v. Centrosphere Indus., 805 F. Supp. 1157, 1197 (D.N.J. 1992) (concerning trade secrets involving pollution control chemicals and related materials).

Reasonable Measures. Trade secrets are also fundamentally different from other forms of property in that the owner of a trade secret must take reasonable measures under the circumstances to keep the information confidential. See 18 U.S.C. § 1839(3)(A). This requirement is generally not imposed upon owners of other types of property. For example, a defendant can be convicted for stealing a bike even if the victim failed to protect it by leaving it unlocked on his front porch. Nevertheless, this requirement was imposed to insure that a person cannot obtain a monopoly on ideas that are in the public domain.

The extent of the security measures taken by the owner of the trade secret need not be absolute, but must be reasonable under the circumstances, depending on the facts of the specific case. See, e.g., Pioneer Hi-Bred Int'l v. Holden Found. Seeds, 35 F.3d 1226, 1236 (8th Cir. 1994) (describing steps taken by plaintiff to safeguard genetic messages of its genetically

engineered corn); Gates Rubber Co. v. Bando Chemical Indus., Ltd., 9 F.3d 823, 848-49 (10th Cir. 1993) (describing steps taken by plaintiff to protect industrial belt replacement program software); K-2 Ski Co. v. Head Ski Co., 506 F.2d 471, 473 (9th Cir. 1974) (describing steps taken by plaintiff to protect trade secrets relating to the design and manufacture of high performance skis). "Reasonable efforts" can include advising employees of the existence of a trade secret, limiting access to the information to a "need to know basis," requiring employees to sign confidentiality agreements, MAI Sys. Corp. v. Peak Computer, 991 F.2d 511, 521 (9th Cir. 1993) (describing measures taken by computer system manufacturer to safeguard its trade secrets from computer servicing company), and keeping secret documents under lock and key. 1 Roger Milgrim, Milgrim on Trade Secrets § 1.04 at 1-126 (1994). See also Reingold v. Swiftships, Inc., 126 F.3d 645, 650 (5th Cir. 1997) (holding that evidence probative of secrecy includes precautions taken by the claimant to preserve secrecy, the willingness of licensees to pay for disclosure of the secret, unsuccessful attempts by the defendant or others to duplicate the information by proper means, and resort by a defendant to improper means of acquisition).

Each trade secret owner must assess the value of the protected material and the risk of its theft when devising reasonable security measures. Under this principle, prosecutors must be able to establish that the security measures used by the victim to protect the trade secret were reasonably commensurate with the value of the trade secret. For example, prosecutors should determine the extent of the security used to protect the trade secret, including physical security and computer security, as well as the company's policies on sharing information with third-parties, including sub-contractors and licensed vendors. If investigation reveals, for example, that any low-level employee in a very large company could gain access to the information, it might not qualify as a trade secret.

Courts have held that information may remain a trade secret even if the owner discloses the information to its licensees, vendors, or third parties for limited purposes. See, e.g., Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174 (7th Cir. 1991) (holding that fact issue whether manufacturer took reasonable precautions to protect its trade secrets in its piece part drawings used to manufacture replacement parts precluded summary judgement). The owner of the trade secret must, however, take reasonable security measures when it discloses the information, such as requiring non-disclosure agreements from all recipients of the information. Further, a trade secret can lose its protected status if it is disclosed, for example, either through legal filings (such as by the issuance of a patent),[14] or through accidental or intentional disclosure

[14] A process or device that is patented can not be a trade secret after the patent has been issued. Upon publication of the patent, the process is publically available for all to see, but the owner enjoys patent protection against another company's use of the technology. In many circumstances, however, subsequent refinements and enhancements of the technology described in the patent may qualify as trade secrets so long as they are not reasonably ascertainable from the published patent itself. See United States v. Hsu, 185 F.R.D. 192 (E.D. Penn. 1999) ("[A] patent application's disclosure of 'best mode' does not require disclosure of later or more specific refinements of the art."). Finally, during the period when a patent has been submitted,

by an employee at conferences, at trade shows, or in writings. See, e.g., Apollo Techs. v. Centrosphere Indus., 805 F. Supp. 1157, 1198 (D.N.J. 1992) (concerning trade secrets involving pollution control chemicals and related materials) . Courts have differed as to whether information can lose its status as a trade secret through an anonymous posting on the Internet, even for a very limited time. Compare Religious Tech. Ctr. v. Netcom On-Line Communication Servs. Inc., 923 F. Supp. 1231 (N.D. Cal. 1995) (holding that trade secret status was lost when information was anonymously posted to the Internet), with DVD Copy Control Ass'n, Inc. v. McLaughlin, 2000 WL 48512 at *3 (Cal.Superior, Jan 16, 2000) (refusing to deem trade secret status destroyed merely by the posting of the trade secret to the Internet because "to hold otherwise would do nothing less than encourage misappropriators of trade secrets to post the fruits of their wrongdoing on the Internet as quickly as possible and as widely as possible thereby destroying a trade secret forever").

Disclosures made to the government or to other law enforcement agencies as part of an investigation or prosecution of an EEA case, however, should have no effect on the trade secret status of the materials. This type of disclosure is essential for the investigation and prosecution of illegal activity and is expressly contemplated by the Economic Espionage Act, as several sections of the EEA make clear. First, 18 U.S.C. § 1835 specifically 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 other applicable laws." 18 U.S.C. § 1835. In fact, under this provision, the government has the right to seek an interlocutory appeal of any court order directing the "disclosure of any trade secret." Id. This section is aimed at protecting the victim's trade secret information during the course of a criminal prosecution. Such protection would be unnecessary unless it was contemplated that victims would first provide the government with the trade secrets for use in the criminal investigation and prosecution. In addition to the protection afforded to trade secret owners by the EEA itself, there are additional restrictions on the disclosure of trade secret information acquired by the Department of Justice for law enforcement purposes without the consent of the trade secret owner or the express written authorization of Senior Officials at the Department of Justice. See, e.g., 28 C.F.R. § 16.21. As a result, trade secret owners who disclose information to law enforcement representatives should not be deemed to have waived trade secret protection. See United States v. Pin Yen Yang, 1999 U.S. Dist. LEXIS 7130 (N.D. Ohio, March 18, 1999) (holding that victim's disclosure of trade secret information 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).

Such reporting to law enforcement is also specifically encouraged by 18 U.S.C. § 1833, which confirms that "[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

---

the information contained in the patent application may qualify as a trade secret so long as the application itself has not been published by the patent office.

respect to that violation." The inclusion of this section, together with 18 U.S.C. § 1835, demonstrates that Congress intended to ensure that someone who becomes aware of an EEA violation has no disincentive to report criminal activity to law enforcement. If disclosures to law enforcement, whether by the owner of a trade secret or a third-party, eliminated trade secret protection, Congressional intent would be frustrated.[15] Therefore, it is unnecessary for federal prosecutors or law enforcement agents to sign protective orders with victims before accepting trade secret information.

Independent economic value. Finally, the trade secret must derive "independent economic value . . . from not being generally known to . . . the public." 18 U.S.C. § 1839(3)(B). Since the EEA does not require that the government prove a specific jurisdictional amount, proving this element should not be difficult.

As discussed below in the section on valuation, the value of the trade secret need not be established with precision and can be determined through a variety of different methods, including: (1) the amount similar trade secret information sold for on the legitimate open market, if available; (2) a reasonable royalty calculation based on what a willing buyer would pay a willing seller for the technology in an arms-length transaction; (3) the amount of research and development costs expended by the trade secret owner; and, (4) as a last resort, the thieves' market price that the defendant actually received or paid in exchange for the technology.

Customer lists. Not all information that a company deems to be proprietary will satisfy this element. For example, under the similar definition of trade secrets found in the Uniform Trade Secrets Act, courts generally have found that customer lists should be considered trade secrets only where the customers are not known in the particular industry, the customers can be discovered only by extraordinary efforts, and where the customer list has been developed through a substantial expenditure of time and money, providing its owner with independent economic value because the information is not known to the general public. See Electro Optical Indus., Inc. v. White, 76 Cal. App.4th 653, 685 (1999) ("[W]here many firms are potential customers for a product but only a few actually purchase it, their identities have economic value to all suppliers of the product because compiling a list of actual customers requires an investment of time and money"); Leo Silfen, Inc. v. Cream, 278 N.E.2d 636, 639-41 (N.Y. 1972) (listing factors). Conversely, where the identities of the customers are readily ascertainable outside the list owner's business, and the compilation of the list was merely the result of general marketing efforts, courts have been less inclined to afford the lists trade secret status. See Standard Register Co. v. Cleaver, 30 F. Supp.2d 1084, 1095 (N.D.Ind. 1998) (holding that list was not a trade secret where owner's competitors knew customer base, knew other competitors quoting the work, and

---

[15] See United States v. Hsu, 185 F.R.D. 192, 199 (E.D. Pa. 1999) (momentary disclosure of trade secret information by government to defendant as part of sting does not waive trade secret protection because "to hold that dangling such bait waives trade secret protection would effectively undermine the Economic Espionage Act at least to the extent that the Government tries, as here, to prevent an irrevocable loss of American technology before it happens").

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 where base of potential customers was neither fixed nor small).

If a prosecutor is contemplating charging a customer list case under the Economic Espionage Act, he or she is advised to contact the Computer Crime and Intellectual Property Section for further consultation and guidance.

3. Additional 18 U.S.C. § 1831 element: intent to benefit a foreign government, foreign instrumentality, or foreign agent

The second mens rea requirement of a 18 U.S.C. § 1831 violation is that the defendant intended or knew that the offense would "benefit" a "foreign government, foreign instrumentality, or foreign agent." The term "foreign instrumentality" means: "any agency, bureau, component, institution, association, or any legal, commercial, or business organization, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government." 18 U.S.C. § 1839(1). The term "foreign agent" means: "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 a foreign entity. When this "entity" is not, per se, a government entity (e.g., a business), there must be evidence of foreign government sponsorship or "coordinated intelligence activity." 142 Cong. Rec. S12201, S12212 (daily ed. Oct. 2, 1996).

The legislative history of the EEA indicates that "benefit" is to be interpreted broadly and is not limited to an economic benefit, but includes a "reputational, strategic, or tactical benefit." H.R. Rep. No. 788, 104th Cong., 2d Sess. (1996).

The requirement that the benefit accrue to a foreign government, instrumentality or agent should be very carefully analyzed by government prosecutors. In order 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). The EEA does not define "substantially," but its use suggests that the prosecution does not have to prove complete ownership, control, sponsorship, command, management or domination. The legislative history states:

> 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. S12201, S12212 (daily ed. Oct. 2, 1996).

Thus, § 1831 does not apply where a foreign corporation misappropriates the trade secret and there is no evidence of sponsorship or "coordinated intelligence activity" by a foreign government. Id. at S12213. In such an instance, however, the foreign corporation could still be properly charged under 18 U.S.C. § 1832. Through October 1, 2000, there have not been any cases brought under 18 U.S.C. § 1831. For questions relating to charges under § 1831, contact the Internal Security Section at the Criminal Division at (202) 514-1187.

4. Additional 18 U.S.C. § 1832 elements

a. Economic benefit to a third party

Under 18 U.S.C. § 1832, the government must prove that the act of misappropriating the trade secret was intended for the economic benefit of a person other than the rightful owner (which can be the defendant, a competitor of the victim, or some other person or entity). This differs from 18 U.S.C. § 1831 where foreign government activity is required, and the benefits may be non-economic. Therefore, a person 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.

b. Intent to injure the owner of the trade secret

Beyond demonstrating that the defendant both knew the information taken was proprietary and intended that the misappropriation economically benefit someone other than the rightful owner, the government in an 18 U.S.C. § 1832 case must also prove a third mens rea element: that the defendant intended to "injure" the owner of the trade secret. According to the legislative history of the EEA, 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. 788, 104th Cong., 2d Sess. 1996.

By definition, in order for a trade secret to have value, it must confer a commercial advantage to the owner. Once the information is disclosed to another for the recipient's benefit, the trade secret loses its value. Accordingly, in many cases, establishing this element may not require additional evidence beyond that required to establish that the defendant acted for the economic benefit of someone other than the owner. For example, when a trusted employee of a computer chip manufacturer steals a prototype chip and conveys it to a known direct competitor of the owner, the disclosure of the information to the competitor may be sufficient circumstantial evidence to establish the requisite intent. See, e.g., United States v. Martin, No. 00-1039, 2000 WL 1376377, at *7 (1st Cir. Sept. 28, 2000) (holding that evidence sufficiently established intent to injure when recipient of information had contemplated opening a competing lab and had asked insider to plan to compete with victim's testing methods). In other circumstances, however,

intent to injure may become more significant. For example, if a bank employee steals a customer list (assuming that the list would otherwise qualify as a trade secret) from a bank in order to solicit the bank's mortgage customers to attend a personal empowerment seminar sponsored by the bank employee, it is not self-evident that the employee intended to injure the bank, even though he was acting for his own economic benefit.

c. Product produced for or placed in interstate or foreign commerce

This element requires the government to 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. This element encompasses two issues: that the trade secret be related to a product, and that the product was produced for or placed in interstate or foreign commerce. The requirement that there be a nexus to interstate or foreign commerce appears merely designed to justify federal jurisdiction and can be satisfied in most cases. For example, where the trade secret is related to a product actually being manufactured and sold, this element would be easily established by evidence of interstate sales. Where a product is still in the development phase but is being developed to be sold in interstate commerce, the victim's intent to distribute the product in the future can be adequately demonstrated either by direct witness testimony or by documentary evidence describing the intended goals of the project.

It is possible that a defendant might argue that products still in the research and development stage are not yet being "produced for interstate commerce" because such items are not yet being "produced" for sale. This argument should not be persuasive. If this argument were to prevail, much of the protection of the EEA would be lost, since a trade secret is often most valuable during the development phase. Once the product embodying the trade secret is released to the public, the value of the trade secret is often lost because the product can be examined and the trade secret obtained or deduced.

The implied distinction between products and services contained in this element can be a difficult one to maintain. Although there is no discussion of the "product" requirement in the legislative history, the use of the term "product" appears to exclude pure services, such as technical skills and know-how not embodied in a saleable, transportable good. Distinguishing between a "pure service" and a "product," however, is not an easy task. An example of a "pure service" might be the services of an individual chiropractor who has developed a secret technique for manipulating a patient's spine to reduce or eliminate back pain. If there is no evidence that the chiropractor is developing or has developed a medical product utilizing this secret, but merely uses it in private practice, the theft of this technique by someone who has worked with the doctor, or even by someone who has broken into the doctor's office and pilfered files does not appear to violate the terms of the statute. On the other hand, many "services" are packaged and sold across state lines much like products. For example, the product of a cellular telephone company may be a package consisting of 600 minutes of air-time per month, caller ID, voice mail, paging and messaging units, all of which is accompanied by a "free" telephone. If a

cellular telephone 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 telephone service should not necessarily preclude a prosecution under the EEA.

The most reasonable explanation of the origin of the product requirement is derived from passages of legislative history indicating that the statute is not designed to apply "to innocent innovators or to individuals who seek to capitalize on their lawfully developed knowledge skill or abilities." As the House-Senate Conference report states:

> A prosecution under this statute must establish a particular piece of information that a person has stolen or misappropriated. 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. Thus, the government cannot prosecute an individual for taking advantage of the general knowledge and skills or experience that he or she obtains or comes by during his tenure with a company.

142 Cong. Rec. S12201-03, S12213 (daily ed. Oct. 2, 1996). While the product requirement is not explicitly mentioned in the text, the passage provides support for the notion that skill, as opposed to a particular proprietary piece of information, should not form the basis of a prosecution. Accordingly, while the product requirement should not be interpreted to require a tangible item, theft of information relating to services that are based entirely on personal skills are likely to be excluded under this statute.

5. Attempts and conspiracies

As noted, the statute also prohibits attempts and conspiracies to misappropriate trade secrets. The nature of the elements required to prove these inchoate offenses was the subject of the only appellate decision thus far under the EEA. In United States v. Hsu, 155 F.3d 189 (3d Cir. 1998), the defendants were charged with attempting and conspiring to steal the techniques for manufacturing Taxol, an anti-cancer drug, from Bristol Meyers-Squibb. The Third Circuit heard an interlocutory appeal from a district court order compelling the government to disclose to the defendants the very trade secrets that were the subject of the EEA charges, based on the district court's opinion that the defendants were entitled to have the opportunity to demonstrate that the materials were not trade secrets. In vacating the district court's order, the Third Circuit held that for cases involving charges of attempt or conspiracy under the EEA, the government does not have to prove the existence of an actual trade secret, but, rather, that the defendants believed that the information they were seeking were trade secrets.

As discussed above, this holding should not require the government to show that the defendants consulted a lawyer who drew the legal conclusion that the documents were trade

secrets. Rather, it should be sufficient to show that the defendant knew or firmly believed that the information was valuable to its owner because it was not generally known to the public and also that the owner had taken measures to protect it.

In so holding, the court reasoned that an attempt charge under the EEA requires proof of the same elements used in other modern attempt statutes, including the Model Penal Code. Therefore, a defendant is guilty of attempting to misappropriate trade secrets if, "acting with the kind of culpability otherwise required for commission of the crime, he . . . purposely does or omits to do anything that, under the circumstances as he believes them to be, is an act or omission constituting a substantial step in a course of conduct planned to culminate in his commission of the crime." Model Penal Code § 5.01(1)(c) (1985). In short, the defendant must (1) have the intent needed to commit a crime defined by the EEA, and (2) perform an act amounting to a "substantial step" toward the commission of that crime. Hsu, 155 F.3d at 202.

Based on these elements, the court explained that the government need not prove the existence of an actual trade secret, since "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, the government can satisfy its burden under 18 U.S.C. § 1832(a)(4) by proving beyond a reasonable doubt that the defendants sought to acquire information that they believed to be a trade secret, regardless of whether the information actually qualified as such.

The Third Circuit also rejected the defendants' contention that disclosure of the trade secrets was required by a potential legal impossibility defense to charges of attempt and conspiracy under the EEA. The court first recognized that the Third Circuit was the only circuit court in the United States that still recognized a common law defense of legal impossibility to attempt charges. Although the Third Circuit had established the defense's validity for certain attempt crimes in United States v. Berrigan, 482 F.2d 171, 190 (3d Cir. 1973), it subsequently limited Berrigan's reach by recognizing several exceptions to the rule where the criminal statute at issue evidenced Congress' intent to foreclose an impossibility defense. See, e.g., United States v. Everett, 700 F.2d 900, 908 (3d Cir. 1983) (holding that legal impossibility was no defense to the charge of attempted distribution of a controlled substance).

The court summarily rejected the viability of a legal impossibility defense to the conspiracy charge, holding that because it is the conspiratorial agreement itself, and not the underlying substantive acts, that forms the basis for conspiracy charges, the impossibility of achieving the goal of a conspiracy is irrelevant to the crime itself. See Hsu, 155 F.3d at 203, (citing 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).

The court examined the EEA's legislative history and concluded that, like the drug statute at issue in Everett, Congress did not intend to permit a defense of impossibility to an "attempt" crime under the EEA: "the 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." Hsu, 155 F.3d at 202.

The court also found it significant that the 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 forced to use actual trade secrets during undercover operations. The court then noted that this requirement 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, based on the legislative intent, and given the practical import of a contrary finding, 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).

Since the Third Circuit decision in the Hsu case, the only district court to consider the question of the required elements for attempt and conspiracy charges has followed Hsu's holding. See United States v. Pin Yen Yang, 1999 U.S. Dist. LEXIS 7130 (N.D. Ohio, Mar. 18 1999) ("[N]either conspiracy nor attempt to violate the EEA requires proof that the information sought to be obtained was actually a trade secret. The government need only demonstrate that the Defendants believed that the information they attempted to acquire was a trade secret.").

6. Potential defenses

a. Parallel development

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 the trade secret. Other companies and individuals have the right to discover the elements of a trade secret through their own research and hard work. Thus, there is no misappropriation if a defendant demonstrates that he independently developed information that constitutes another's "trade secret."

b. Reverse engineering

Similarly, a person can legally discover the elements of a trade secret by "reverse engineering": the practice of taking something apart to determine how it was made or manufactured. See, e.g., Kewanee Oil Co., 416 U.S. at 476 (stating that the law does not protect the owner of a trade secret from "discovery by fair and honest means, such as independent invention, accidental disclosure, or by so-called reverse engineering"). The EEA does not expressly address when reverse engineering is a valid defense; however, the legislative history suggests that "the 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. S12201, S12212 (daily ed. Oct. 2, 1996).[16]

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 sought 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 Alcatel USA, Inc. v. DGI Techs., Inc., 166 F.3d 772, 784 (5th Cir. 1999) (holding that a competitor could not assert reverse engineering defense where it first unlawfully made 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, 1236 (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, 232 (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 avoid a successful claim by the defendant that he discovered the trade secret by reverse engineering, prosecutors must establish the means by which the defendant misappropriated the trade secret. If the prosecution demonstrates that the defendant unlawfully obtained access to the trade secret, it would refute a defendant's claim that he learned of the trade secret through reverse engineering.

c. General knowledge

As noted, the EEA does not apply to individuals who seek to capitalize on their lawfully developed knowledge, skill, or abilities. Employees, for example, who change employers or start their own companies cannot be prosecuted based on an assertion that they were exposed to a trade secret while employed, unless the government can establish that they stole or misappropriated a particular trade secret. The legislative history makes clear that "[t]he government can not prosecute an individual for taking advantage of the general knowledge and skills or experience that he or she obtains or comes by during his tenure with a company. Allowing such prosecutions to go forward and allowing the risk of such charges to be brought would unduly endanger legitimate and desirable economic behavior." 142 Cong. Rec. S12201, 12213 (daily ed., Oct. 2, 1996). This does not mean, however, that employees who leave their employers to start their own companies can never be prosecuted under the EEA. In cases where employees steal or without authorization appropriate a trade secret from their employer, they may be prosecuted under 18 U.S.C. § 1832, assuming, of course, that the other elements can also be

---

[16] By contrast, the prohibition on circumvention of copyright protection systems, 17 U.S.C. § 1201(a), does have an explicit albeit limited exception for reverse engineering. See 17 U.S.C. § 1201(f). See also supra Section V.C.1 at page 76 (discussing protections for copyright protection systems).

satisfied. Clear 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." However, where the actions of a departing former employee are unclear and evidence of theft has not been discovered, it may be advisable to allow the company to pursue its civil remedies and make a subsequent referral, if additional evidence of theft is developed.

d. The First Amendment

In most instances, if the government can establish that the defendant intended for the misappropriation to benefit a third party economically, the defendant should not be able to claim successfully that the First Amendment of the Constitution protected the disclosure of the trade secret. In other words, if the defendant's motivation was pecuniary, the defendant cannot very well argue that he disclosed the secret as a public service or to educate the public. Further, courts also have rejected a First Amendment defense if the speech itself is the very vehicle of the crime. See, e.g., United States v. Morrison, 844 F.2d 1057, 1068 (4th Cir.) (rejecting defendant's First Amendment defense, upholding a conviction for a violation of 18 U.S.C. § 641 for stealing secret government documents, and noting that, "[w]e do not think that the First Amendment offers asylum . . . just because the transmittal was to a representative of the press"), cert. denied, 488 U.S. 908 (1988); United States v. Rowlee, 899 F.2d 1275 (2d Cir.) (rejecting assertion of First Amendment protection in tax evasion conspiracy case), cert. denied, 498 U.S. 828 (1990). Additionally, in United States v. Riggs, 743 F. Supp. 556, 560-61 (N.D. Ill. 1990), the court rejected defendant's assertion that the First Amendment provides a 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 [defendant's] argument that the criminal activities with which he is charged . . . are protected by the First Amendment. Interpreting the First Amendment as shielding [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.

Since a claim of First Amendment protection is irrelevant to the defendant's illegal activities, the government should consider seeking an in limine order precluding the introduction of such evidence in appropriate cases.

e. Advice of counsel or claim of right

The EEA is violated only where someone acts knowingly without authorization. Under certain circumstances, however, two individuals or companies may have a legitimate dispute over ownership rights in a trade secret. This type of dispute is likely to arise where the two potential owners previously worked together to develop the disputed technology and where the contractual arrangements governing each party's respective ownership interests are unclear or entirely

absent. In these circumstances, unilateral action with regard to the trade secret by one of the owners may precipitate an EEA criminal referral. Such cases are rarely appropriate for criminal prosecution, especially where the party taking unilateral action has obtained advice of counsel. Notwithstanding the passage of the EEA, many disputes regarding ownership of intellectual property, including trade secrets, continue to be best resolved in a civil forum.

f. Statutory challenges

Several of the defendants in the first twenty cases brought under the EEA have attempted to challenge the statute, alleging, among other claims, that various provisions are vague or otherwise unconstitutional. Thus far, all such challenges have been rejected. Of these challenges, however, only United States v. Hsu, 40 F. Supp.2d 623 (E.D. Pa. 1999) (a challenge leveled after the remand from the Third Circuit) resulted in a published opinion.

In Hsu, the defendant moved to dismiss charges of conspiracy to steal and attempted theft of trade secrets, asserting that the EEA is unconstitutionally vague in two respects: (1) it fails to define the term "related to or included in" a product that is produced for or placed in interstate or foreign commerce and (2) the definition of "trade secret" in 18 U.S.C. § 1839(3) offends due process with its vagueness because it does not define either "reasonable measures" to keep the information secret, or what is meant by information not being "generally known" or "readily ascertainable" to the public. See 18 U.S.C. § 1839(3).

In denying the motion, the court noted that the void for vagueness doctrine does not mean that a statute is unconstitutionally vague where "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. The court also held that since the First Amendment was not implicated, Hsu's void for vagueness challenge could only succeed if the statute were vague as applied to his conduct and not based on some hypothetical case. Id. The court summarily rejected Hsu's claim that free expression issues were implicated because the Bristol-Meyers Squibb employee who aided the Government "sting" operation by posing as a corrupt employee has a right to freely express himself and exchange information with the defendant, or with anyone else he thinks is a potential employer. The court noted first that Hsu lacked standing to raise the employee's First Amendment rights claim, and that even if Hsu had standing, the employee had knowingly participated in a Government sting operation, not in a job interview with a potential employer. Therefore, no First Amendment interests were implicated.

The court then 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. The court found that 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 where, as here, the defendant was well versed in 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 prong of the definition mandating that the owner take "reasonable measures" to keep the information secret, the court dismissed the argument that the mere use of the word "reasonable" or "unreasonable" renders a statute vague. Id.[17] The court observed that the defendant was told on several occasions that the Taxol technology in question was proprietary to Bristol-Meyers Squibb, could not be acquired via a license or joint venture, and could only be obtained through an allegedly corrupt employee. Hsu thus knew that Bristol-Meyers Squibb had taken many steps to keep its technology secret, and therefore could not contend that the "reasonable measures" was vague as applied to him in this case.

Finally, the court concluded that the aspect of the trade secret definition requiring that the information not be "generally known to" or "readily ascertainable by" the public did not render the EEA void for vagueness. Notably, the court found the EEA's use of the terms 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, the court reasoned that evidence of Hsu's e-mails, telephone calls, and conversations showed a pattern whereby Hsu believed that the information he was seeking could not be acquired through legal or public means. Therefore, the court concluded that the definition of trade secret as applied to Hsu was not unconstitutionally vague.

7. Criminal forfeiture

The EEA also provides that the court imposing sentencing shall order the forfeiture of any proceeds or property derived from violations of the EEA, and may order the forfeiture of any property used to commit or to facilitate the commission of the crime. The statutory language of the first subsection is mandatory and leaves the judge no discretion. See 18 U.S.C. § 1834(a)(1). With regard to the latter provision, however, the court may in its discretion take into consideration "the nature, scope, and proportionality of the use of the property in the offense." 18 U.S.C. § 1834(a)(2). The intent of that limitation is to insure that the amount and character of the forfeited property is proportionate to the harm caused by the defendant's conduct.

In the early cases prosecuted under the EEA, discretionary forfeiture has been sought for computer systems owned by the defendant and used to store and transfer trade secrets belonging to the victim. As a procedural matter, indictments alleging a violation of either 18 U.S.C. § 1831 or § 1832 should contain, where appropriate, a forfeiture paragraph. For additional discussion of forfeiture in intellectual property infringement cases, see supra Section VII.C at page 120.

---

[17] The court further recognized that this aspect of the definition is taken, "with only minor modifications," from the definition used in the Uniform Trade Secret Act (UTSA), which has been adopted in forty states and the District of Columbia, and the language of which has withstood a vagueness attack.

8. Civil proceedings

While the EEA does not provide for civil forfeiture proceedings, it does authorize 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 the trade secret while conducting a criminal investigation or in cases in which a defendant's conduct does not warrant criminal prosecution. Prosecutors should also consider using this portion of the statute, in combination with consent decrees, to enjoin any third-party recipients of the trade secret from distributing or making use of the trade secret materials.

9. Confidentiality and the use of protective orders

Victims of trade secret thefts are often faced with a dilemma when deciding whether to report the matter to law enforcement authorities. Generally, victims do not want the thief to go unpunished but are concerned that if they report the matter, the trade secret will be disclosed during discovery or during the criminal trial. In drafting the EEA, Congress recognized this issue and, to encourage reporting, sought to preserve the confidentiality of trade secrets, if possible, throughout the prosecution. The EEA provides that the court "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. This section also provides for interlocutory appeals from a decision or a court order authorizing the disclosure of any trade secret. Id. Therefore, prosecutors are strongly encouraged to seek the entry of orders that will preserve the status of the information as a trade secret and prevent its unnecessary and harmful disclosure.

A variety of steps may be taken to protect the confidentiality of information. Among the solutions employed in the first cases brought under the EEA were: protective orders during discovery, redacted documents, sealed exhibits, and the use of courtroom video monitors to display documents to the court and jury but not the public.

On at least one other occasion, a courtroom has been sealed during the sentencing phase of the proceeding to avoid disclosure of proprietary business information relating to the damages caused by the theft of trade secrets.[18] Prosecutors should be aware of the procedures in the

---

[18] Note that courts can limit the disclosure of information to the public even during the trial without necessarily violating the defendant's right to a public trial under the Sixth Amendment. While the right to a public criminal trial was incorporated into the Constitution by the Sixth Amendment, the right is not absolute and may be limited in certain circumstances. See Richmond News Papers, Inc. v. Virginia, 448 U.S. 555, 599-600 (1980) (Stewart, J. concurring); see also Gannett v. Depasquale, 443 U.S. 368, 422-33 (1979) (Marshall, 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-

federal regulations and Department of Justice guidelines requiring approval of the Deputy Attorney General before requesting that a courtroom be sealed. See 28 C.F.R. § 50.9; U.S. Attorneys' Manual § 9-5.150. Whenever authorization to close a judicial proceeding is being sought pursuant to 28 C.F.R. § 50.9 in a case or matter under the supervision of the Criminal Division, the Policy and Statutory Enforcement Unit, Office of Enforcement Operations should be contacted. In cases or matters under the supervision of other divisions of the Department of Justice, the appropriate division should be contacted. The Office of Enforcement Operations may be contacted at (202) 514-3684.

Prosecutors should continue to seek to use these procedures and other measures to limit the potential for disclosures of trade secrets throughout the criminal proceeding in the most appropriate manner.

Protective orders have been utilized in several EEA cases and their use was expressly sanctioned by the Third Circuit in the Hsu decision described above. The dispute in Hsu centered around the government's motion for a protective order pursuant to 18 U.S.C. § 1835 and Fed. R. Crim. P. 16(d)(1) that would have permitted the government to disclose to the defendants only redacted versions of the documents used in the EEA sting operation and the defendants' opposing request for unredacted copies of the same documents. The proposal advanced by the defendants required the government to provide the trade secret information to the defendants, their attorneys and their experts under a protective order that restricted the use of the documents to the criminal litigation and would have required the return or destruction of the documents at the end of the case. The district court's decision to adopt the defendants' version of the order precipitated the interlocutory appeal of the United States. See United States v. Hsu, 982 F. Supp. 1022 (E.D. Pa. 1997).

On appeal, the Third Circuit determined that 18 U.S.C. § 1835 of the EEA clearly demonstrates Congress' intent to protect the confidentiality of trade secrets to the fullest extent possible under the law. Hsu, 155 F.3d at 196. While recognizing that such protection does not abrogate existing constitutional and statutory protections for criminal defendants, the court held that the government's proposed order did not violate the defendants' constitutional rights under the facts of the case 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.[19] As to the defendants' claim that the trade secrets

---

67 (Wis. 1983) (citing State ex rel. Ampco Metal, Inc. v. O'Neil, 78 N.W.2d 921 (Wis. 1956)) (both discussing inherent power of a court to limit the public nature of trials).

[19] 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 a "complex issue," noting that the definition of trade secret expressed in the EEA "raise[s] an issue as to whether the information or formula itself is in fact material to the existence of the trade

were also material to the preparation of other defenses, including entrapment and outrageous government conduct, the court was openly skeptical "of the materiality, let alone relevance, of the redacted information to these issues." Id. at 204. However, because these arguments had been raised for the first time on appeal, the court remanded these issues to the district court. Id.

On remand, the district court rejected the defendants' arguments that they were entitled to received unredacted trade secret documents under Fed. R. Crim. P. 16(a)(1)(C), and found that the unredacted documents were not relevant to the defenses of entrapment and outrageous government conduct. Just as the government need not use actual controlled substances during a drug "sting" operation for a drug defendant to allege that he was induced by the Government and was not predisposed to commit the crime, whether the trade secrets used by the government in an EEA "sting" operation were real or "dummy" secrets has no effect on an entrapment defense. Id. at 198 n.19. The court similarly rejected the defendants' arguments based on the defenses of document integrity and the chain of custody, concluding that these defenses can also be resolved without the objects at issue. Id. at 199. The court also rejected the defendants' argument that the government and Bristol-Meyers waived the confidentiality of the trade secrets when they showed the documents voluntarily during the sting operation. Id.

Finally, after an in camera review by a court-appointed technical advisor who had taken an oath of confidentiality, the court rejected the defendants' argument that if shown the documents in their unredacted form, they could prove that the information contained in the documents was in the public domain. Based on the technical advisor's analysis, 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).[20] After reviewing this category of redactions in camera, and consulting with the expert, the court held that the redactions were properly made to avoid disclosure of trade secret information within the meaning of the Economic Espionage Act. Id. at 200.

Taken together, the Third Circuit's opinion in Hsu and the district court's opinion on remand suggest that courts will recognize and respect the Congressional directive to take appropriate measures to preserve the confidentiality of trade secrets throughout the criminal process.

10. Extraterritoriality

---

secret." Id. at n.15. Thus, the issue of the government's disclosure obligations in a completed offense case has not yet been resolved.

[20] The expert also identified a second category of redactions that in his view were less strictly tied to the practice of the art and did not meet the statutory definition of a trade secret because they did not derive any independent economic benefit or value. Therefore, the court ordered that these portions be disclosed to defendants.

In order to rebut the general presumption against the extraterritoriality of U.S. criminal laws, Congress made it clear that the EEA is meant to apply to specified conduct occurring outside the United States. To ensure that there is sufficient nexus to U.S. interests, the EEA applies to conduct occurring 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. See 18 U.S.C. § 1837.

11. Department of Justice oversight

Prior to the passage of the EEA, the Attorney General assured Congress in writing that for a period of five years, the Department of Justice would require that all prosecutions brought under the EEA must first be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General of the Criminal Division. This requirement has since been codified at 28 C.F.R. § 0.64-5 and is interpreted to apply to the filing of complaints, indictments and civil proceedings, but not to search warrant applications or other investigative measures. Pursuant to this requirement, the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice has been designated to coordinate requests for approval for 18 U.S.C. § 1832 cases. The Internal Security Section coordinates requests for approval for 18 U.S.C. § 1831 cases.

C. Sentencing and Restitution

Because the sentence in an EEA case will be largely driven by the value of the misappropriated property, a sentencing under the EEA can be complex, involving the testimony of both fact and expert witnesses.

1. Offense level

The applicable guideline for violations of 18 U.S.C.§§ 1831 and 1832 is U.S.S.G. § 2B1.1, which specifies a base offense level of four. That base 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. Sentencing Guidelines Manual § 2B1.1(b)(7) (1999). It will often be the case that the offense will also have involved more than minimal planning, mandating another two point increase.

If a defendant is convicted of solely on conspiracy or attempt violations, U.S.S.G. § 2X1.1 instructs courts to decrease the base offense level three 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. Sentencing Guidelines Manual § 2X1.1(b)(1) (1999). In most attempt cases resulting from undercover operations, the three point reduction will not apply.

2. Loss

Under U.S.S.G. § 2B1.1(b)(1), the court shall increase the offense level according to the specific amount of the "loss" inflicted by the theft. Under U.S.S.G. § 2B1.1, "loss" is defined as "fair market value of the property taken, damaged, or destroyed. Fair market value is the appropriate inquiry because the "value of the property taken . . . is an indicator of both the harm to the victim and the gain to the defendant." U.S. Sentencing Guidelines Manual § 2B1.1, cmt. (1999). Where the market value is difficult to ascertain or inadequate to measure harm to the victim, the court may measure loss in some other way, such as reasonable replacement cost to the victim." U.S. Sentencing Guidelines Manual § 2B1.1, app. n.2 (1999). U.S.S.G. § 2B1.1 also instructs that "loss need not be determined with precision. The court need only make a reasonable estimate of the loss given the available information." U.S. Sentencing Guidelines Manual § 2B1.1, app. n.3 (1999).

The only existing case law concerning the proper measure of loss in trade secret cases has arisen from civil cases decided pursuant to the Uniform Trade Secret Act. Despite the large number of such cases, it remains true that "the general law as to the proper measure of damages in a trade secret case is far from uniform." Telex Corp. v. Int'l Bus. Machs. Corp., 510 F.2d 894, 930 (10th Cir. 1975) (concerning allegations of unfair competition and misappropriation of trade secrets and confidential information relating to electronic data processing systems). Instead of offering well-settled rules, these decisions demonstrate that courts tend to exercise broad latitude in measuring damages. Even Section 3 of the Uniform Trade Secrets Act offers several alternative methods that can be employed in such cases:

> 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 Secret Act § 3.

In determining damages under the UTSA, courts vary between determining the market value of the trade secret based on the loss inflicted on the victim or the gain accrued by the defendant, depending on which appears to be either the more reliable or the greater measure given the particular circumstances of the theft. See University Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518 (5th Cir. 1974) (involving computer company's suit for breach of joint venture agreement, misappropriation of plaintiff's computer system, and violation of a noncompetition agreement); Vermont Microsystems, Inc. v. Autodesk Inc., 138 F.3d 449, 452 (2d Cir. 1998) ("[T]he amount of damages recoverable in any action for misappropriation of trade secrets may be measured either by the plaintiff's losses or by the profits unjustly received by the defendant.").

In circumstances where the value of the trade secret to the plaintiff has not been completely destroyed (as often will be the case in the majority of Economic Espionage Act prosecutions) courts determining damages for theft of trade secrets under the Uniform Trade Secret Act have most often focused on the gain to the defendant as the proper measure of market value. In such circumstances, focusing solely on the loss suffered by the defendant would understate the magnitude of the harm suffered and inadequately punish the wrongdoer. If loss to the victim were the only appropriate measure of damages, someone caught red-handed stealing trade secrets could not be punished if the information had not yet been used to the owner's detriment. See 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 Med. 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).

In criminal cases where the defendant may not have yet used the misappropriated trade secret, the gain to the defendant should be measured by the value of the information that the defendant received. This is consistent with the general approach of the Sentencing Guidelines, which state that "loss" is based on the value of the stolen property even where the stolen property is recovered immediately. See U.S. Sentencing Guidelines Manual. § 2B1.1, app. n.2 (1999). This is also consistent with the approach set out in U.S.S.G. § 2X1.1, which indicates that "[i]n an attempted theft, the value of the items that the defendant attempted to steal would be considered." Id. § 2X1.1, app. n.2 (1999). See also id. § 2F1.1, app. n.7 ("Consistent with the provisions of § 2X1.1 (Attempt, Solicitation, or Conspiracy), if an intended loss that the defendant was attempting to inflict can be determined, this figure will be used if it is greater than the actual loss.").

One method commonly used to determine the market value of stolen trade secret information is to calculate the amount the thief would have had to pay in license or royalty fees had he legitimately licensed the stolen technology. This measure of damages is known as the "reasonable royalty approach." Another method is to value the information at what it would have cost the defendants to have developed the information independently, which is usually determined based on the victim's historical research and development costs. This method, known as the "replacement cost" method is endorsed by an application note to U.S.S.G. § 2B1.1 in circumstances where the market value is otherwise difficult to ascertain. See U.S. Sentencing Guidelines Manual § 2B1.1 applic. n.2.

Of these two approaches, in circumstances where the defendant has not yet realized a sufficient profit from the information he stole so as to provide a ready indication of market value, a "reasonable royalty" or "forced licensing" measure of damages should be applied. See Vitor Corp. of Am. v. Hall Chem. Co., 292 F.2d 678, 683 (6th Cir. 1961) ("If actual value can be ascertained by a reasonable apportionment of profits and damages, that course should be pursued. But if this cannot be accomplished, the nature of its invention, its utility, and advantages and

extent of use involved are elements to be considered in determining a reasonable royalty."); see also Vermont Microsystems, Inc., 138 F.3d at 450 (holding that a reasonable royalty should be the measure of damages and that "reasonable royalty is a common form of award in both trade secrets and patent cases"); Uniform Trade Secret Act § 3(a) ("[I]n 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."). Other federal cases in which the "reasonable royalty" approach was used include: Molex, Inc. v. Nolen, 759 F.2d 474 (5th Cir. 1985); University Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518 (5th Cir. 1974); Carter Prods., Inc. v. Colgate-Palmolive Co., 214 F. Supp. 383 (D. Md. 1963).

In Vitor Corp., the Sixth Circuit explained why the reasonable royalty measure of damages most closely determines the value of misappropriated information in cases involving an absence of actual lost profits or sales:

> To adopt a reasonable royalty as a measure of damages is to adopt and interpret as well as may be the fiction that a license was to be granted at the time of the infringement and then to determine what the license price should have been. In effect, the Court assumes the existence ab initio of and declares the equitable terms of a supposition license and does this nunc pro tunc. It creates and applies retrospectively a compulsory license. The primary inquiry is what the parties would have agreed upon if both were reasonably trying to reach an agreement. Pecuniary loss in any event can be determined by reasonable approximation. The actual value of what has been appropriated is always the ultimate in appraisement. If actual value can be ascertained by a reasonable apportionment of profits and damages, that course should be pursued. But if this cannot be accomplished, the nature of the invention, its utility, and advantages and extent of use involved are elements to be considered in determining a reasonable royalty.

Vitor Corp. of America v. Hall Chem. Co., 292 F.2d 678, 682-83 (6th Cir. 1961) (citing Egry Register Co. v. Standard Register Co., 23 F.2d 438 (6th Cir. 1928)).

Because civil trade secret cases generally require the plaintiff to prove the defendant's use of the stolen trade secrets, the "reasonable royalty" measure may be easier to apply because the nature of the defendant's use of the technology has already occurred. In cases where the defendant has not yet manifested his intention to use the stolen technology and there is no readily ascertainable reference for determining a reasonable royalty, this approach may prove more difficult and may unduly prolong or complicate the sentencing process. In such circumstances, it may be preferable to use the "replacement cost" measure. A victim's research and development costs have been used to measure replacement cost in appropriate circumstances in civil trade secret cases. For example, in University Computing, the court noted that using the plaintiff's research and development costs alone were appropriate in cases "where the trade secret was used by the defendant in a limited number of situations, where the plaintiff was not in direct competition with the defendant, where the development of the secret did not require substantial

improvements in existing trade practices, and where the defendant's use of the trade secret had ceased." Id. at 538. Other courts have also adopted this approach to establish the proper measure of "loss" in trade secret cases. See Salsbury Labs. Inc. v. Merieux Labs. Inc., 908 F.2d at 714 (holding that research and development costs for misappropriated vaccine were proper measure of damages). This same approach was adopted in a criminal mail fraud case in United States v. Wilson, 900 F.2d 1350, 1356 (9th Cir. 1990):

> As the district court recognized, the figures [the defendant] advocates are relevant in a market for industrial espionage, but not necessarily in an open market: "In my view stolen information always commands less than legitimate information so I think in terms of market value is has got to be many times higher." Yet the district court was faced with a virtually nonexistent open market. The evidence presented by both Wilson and the Government illustrated the uniqueness of the information and the limited application such information would have, even to one of the few companies who could make any use of it. It was not clearly erroneous for this district court to find that market value was difficult to ascertain in these circumstances. Moreover, we give due deference to the court's decision to measure [the victim's] loss according to the company's development costs and find that the court's computation under a development cost analysis also was not clearly erroneous.

Because the "replacement cost" measure is specifically cited in the Sentencing Guidelines, using the victim's research and development costs should be acceptable in cases where a "reasonable royalty" calculation is impossible or impracticable. In both EEA cases thus far that have involved contested sentencing hearings on the issue of loss, the courts have used some variation of the victim's research and development costs to measure the value of the information taken by the defendants.

3. Restitution

The Mandatory Victims Restitution Act of 1996 ("MVRA"), codified at 18 U.S.C. § 3663A, requires that restitution be made in all sentencing proceedings for convictions of, 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) and (B). For cases specifically 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 greater of the value of the property on the date of its damage destruction or loss, or its value at the time of sentencing, less the value of any part of the property that is returned. See 18 U.S.C. § 3663A(b)(1). Because the physical return of stolen trade secrets will be inadequate in most circumstances to compensate a victim for its damages due to the theft and disclosure of such information, restitution in the amount of the value of the stolen trade secrets will often be required. Under the MVRA, such restitution must be ordered "to each victim in the full amount

of the 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).

Although the Economic Espionage Act had not yet been passed at the time that 18 U.S.C. § 3663A was enacted, the theft of trade secrets should fall under the description of offenses contained in § 3663A. The legislative history of the provision indicates that mandatory restitution is intended to apply to "violent crimes, property and fraud crimes under title 18, product tampering, and certain drug crimes." S. Rep. No. 104-179 (1995) (emphasis added). The sentencing guidelines specifically describe theft as "one of the most basic forms of property offenses." Accordingly, the theft of trade secrets should be a qualifying offense against property for purposes of the mandatory restitution statute. As noted, the mandatory restitution statute also applies for any offense where "an identifiable victim has suffered a physical injury or a pecuniary loss." 18 U.S.C. § 3663A(c)(1)(B). 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 supra Section VII.B at page 115.

D. Other Possible Charges

Theft of trade secrets and other proprietary information may violate a number of federal criminal statutes in addition to or instead of 18 U.S.C. §§ 1831-1832. Statutes commonly worth considering are: unlawfully accessing a protected computer to obtain information, 18 U.S.C. § 1030(a)(2); wire or mail fraud including the disclosure of information in violation of a confidential or fiduciary relationship, 18 U.S.C. §§ 1341, 1343, 1346; and the misappropriation and interstate transportation of property or goods, 18 U.S.C. §§ 2314-2315. Prosecutors should consider these other statutes as well as the EEA, 18 U.S.C. §§ 1831-1832. Charging both a violation of the Economic Espionage Act and another statute such as Interstate Transportation of Stolen Property or Wire Fraud arising from the same act or acts does not violate the Double Jeopardy Clause of the Fifth Amendment of the Constitution since "each offense contains an element not contained in the other." United States v. Dixon, 509 U.S. 688, 690 (1993) (citing Blockburger v. United States, 284 U.S. 299, 304 (1932)).

If prosecutors decide not to pursue a case federally, they should consider referring the case to state authorities for prosecution. Many states have laws that specifically address the theft of information, and even if a state does not have such a law, a defendant may often be successfully prosecuted under a more general theft statute.

1. Obtaining information or committing fraud by means of a protected computer, 18 U.S.C. § 1030

In many cases of misappropriated proprietary information, the defendant acquired information by unauthorized access to a computer. In such cases, prosecutors should consider

charging the defendant with a violation of 18 U.S.C. § 1030(a)(2)(A)-(C). Paragraph (A) is violated if the information is a financial record; paragraph (B) if the information was from any federal department or agency; and paragraph (C) if the information came from any "protected computer," as defined at section 1030(e)(2), and if the conduct involved an interstate or foreign communication. A protected computer is a computer used in interstate or foreign commerce or communication, or one used by a financial institution or the United States government exclusively (or in part, if the offense affects that use). 18 U.S.C. § 1030(e)(2).

"Information" as used in this subsection is to be broadly construed and includes information stored in intangible form. Moreover, the phrase "obtaining information" includes merely reading it – there is no requirement that the information be printed out, copied or transported. This is important because, in an electronic environment, information can be "stolen" without transportation, and the original usually remains intact.

Violating 18 U.S.C. § 1030(a)(2) is a misdemeanor if the government does not prove any aggravating factors. 18 U.S.C. § 1030(c)(2)(A). This section does not require that the information obtained be confidential or secret in nature. Violating 18 U.S.C. § 1030(a)(2) is a felony if the government can prove that the offense was committed for financial, commercial, tortious or criminal purposes, or if the information can be valued at greater than $5,000. See 18 U.S.C. § 1030(c)(2)(B).

Prosecutors may also consider section 1030(a)(4), which is intended to provide punishment for those who misuse computers in schemes to defraud victims of property. This felony proscribes an individual from, knowingly and with intent to defraud, accessing a protected computer without authorization, or exceeding authorized access, and by means of such conduct furthering the intended fraud and obtaining anything of value, unless the object of the fraud and the thing obtained is computer time worth less than $5,000.

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

The mail and wire fraud statutes can also be used to prosecute misappropriation of proprietary information. For a more detailed discussion of 18 U.S.C. §§ 1341 and 1343, readers may refer to Chapter 43 of the U.S. Attorney's Manual and may contact the Fraud Section of the Criminal Division at (202) 514-7023 for further information and guidance. See also supra Section VI.B.1 at page 94 (discussing advantages and disadvantages of charging mail and wire fraud in infringement cases).

The federal wire and mail fraud statutes proscribe the use of the mails or of interstate or foreign wire transmission, in furtherance of any scheme to defraud, or any scheme for obtaining "property" by false pretenses or representations. Appellate courts have upheld convictions under these statutes for the theft of trade secrets even where no violation of 18 U.S.C. § 2314 was found. See, e.g., Abbott v. United States, 239 F.2d 310 (5th Cir. 1956) (upholding defendant's conviction for use of mails to defraud in case involving illicit procurement of copies of oil

company's geophysical maps). The broader scope results from the use of the word "property" in the mail and wire fraud statutes as compared to the far narrower phrase "goods, wares and merchandise" used in § 2314. Courts have held that "property" includes intangible property, such as proprietary information.[21] By contrast, at least one appellate court has held that intangible property does not qualify as goods, wares or merchandise for § 2314. See United States v. Brown, 925 F.2d 1301 (10th Cir. 1991); see also Section VIII.D.4 at page 155 (discussing Brown in analysis of applicability of interstate transportation of stolen property charge to trade secret theft). Thus, these statutes provide a basis for prosecution when mails or wires are used in a misappropriation scheme. The mail and wire fraud statutes have been identically construed with respect to the issues discussed here. See, e.g., United States v. Von Barta, 635 F.2d 999, 1005 n.11 (2d Cir.) (reversing lower court's ruling and holding among other things that defendant's conduct in a securities scheme subjected him to prosecution for mail and wire fraud), cert. denied, 450 U.S. 998 (1981).

For example, in United States v. Seidlitz, 589 F.2d 152 (4th Cir.), cert. denied, 441 U.S. 922 (1979), the defendant used his knowledge of his former employer's computer system to enter the computer system and download computer data. The appellate court upheld the trial court's determination that the stolen data qualified as property within the meaning of the wire fraud statute. The court held that the data was a trade secret, even though similar information was in the public domain, because defendant's former employer had "invested substantial sums" to modify the system for its own needs. Further, the information had competitive value, and the employer took steps to prevent persons other than clients and employees from using the system. Id. at 160. Accordingly, there was sufficient evidence from which a jury could conclude that information stored in the computer system was "property" as used in 18 U.S.C. § 1343.

Prosecutors also should consider the applicability of the restored "intangible rights theory" found in 18 U.S.C. § 1346 for charging a defendant with fraudulent misappropriation of trade secret under §§ 1341 or 1343. Section 1346 was enacted in the wake of McNally v. United States, 483 U.S. 350 (1987), where the Supreme Court held that the mail fraud statute did not include schemes to defraud citizens of their intangible right to honest government, but was limited to protecting "property" rights. In a case under 18 U.S.C. § 1346, the defendant is charged not with fraudulently obtaining proprietary information, but rather with breaching the fiduciary duty of loyalty he owes to his employer by misappropriating the proprietary

---

[21] See, e.g., Carpenter v. United States, 484 U.S. 19 (1987). The defendant in Carpenter wrote the "Heard on the Street" column for The Wall Street Journal. Although these columns contained no insider information, they had the potential to affect the stock prices of companies discussed in the column because of the "quality and integrity" of the information. The defendant was charged with passing advance information on the columns to two co-conspirators who executed pre-publication trades and earned profits of $690,000. The Supreme Court held that the defendant had violated the wire fraud statute because the rightful owner of the information contained in the columns had been deprived of its right to the exclusive use of the information. 484 U.S. at 26.

information. Under this theory, the government must prove that the defendant took steps to actively conceal the misappropriation. The United States is not, however, required to prove that the defendant realized any financial gain from the theft or attempted theft.

Illustrative of this theory is United States v. Kelly, 507 F. Supp. 495 (E.D. Pa. 1981), in which the two defendants were charged with mail fraud for unauthorized use of their company's computer time and storage facilities for the development of a private business venture. The jury found that the defendants defrauded Univac of their loyal and faithful services as employees, and used the mails in furtherance of their scheme. The court denied the defendants' post-trial motions arguing that their convictions should be overturned because the government failed to prove that the goal of the fraudulent scheme was to obtain money or some tangible property right from Univac. The court noted that a private employee may be convicted for mail fraud for failure to render honest and faithful services to his employer if he devises a scheme to deceive, mislead, or conceal material information. The evidence that the defendants violated company policy by extensively using their employer's computer facilities for their own gain, in combination with the steps they took to conceal their use from their employer, was sufficient to sustain the conviction.

3. Disclosing government trade secrets, 18 U.S.C. § 1905

Section 1905 statute provides for misdemeanor penalties for government employees who, inter alia, "divulge" or "disclose" government trade secrets. In the only reported decision involving the disclosure of confidential government information, the court in United States v. Wallington, 889 F.2d 573 (5th Cir. 1989), upheld the defendant's conviction for running background checks on several people who a friend of the defendant suspected of drug dealing.

4 Interstate transportation or receipt of stolen property, 18 U.S.C. §§ 2314, 2315

The Interstate Transportation of Stolen Property Act ("ITSP"), 18 U.S.C. § 2314 imposes criminal liability on:

> Whoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud.

See U.S. Attorney's Manual. §§ 9-61.260 - 9.61.261(A-D). 18 U.S.C. § 2315 addresses receiving stolen property, making it a crime to "receive, possess, conceal, store, barter, sell, or dispose" such property. In all other respects 18 U.S.C. §§ 2314 and 2315 are substantively identical.

In a proprietary information case, a prosecutor should prove the first element, the transportation in interstate commerce, in the same manner as with any other stolen goods, wares

or other merchandise case, i.e., by establishing that valuable proprietary information was transported across state lines.

The statute does not define the terms goods, wares or merchandise and courts are divided on under what circumstances intangible property such as trade secrets constitutes "goods, wares or merchandise." In one case, the court dismissed the indictment for transporting the source code of a computer program from Georgia to New Mexico. United States v. Brown, 925 F.2d 1301 (10th Cir. 1991). The government admitted it could not prove either that the defendant copied the source code onto the company's diskettes or that the defendant had in his possession any tangible property belonging to the company. Id. at 1303. The Brown court held that "[p]urely intellectual property," such as the source code appropriated by the defendant, is not covered by 18 U.S.C. § 2314: "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 which have been stolen, converted or taken within the meaning of § 2314 or 2315." 925 F.2d at 1307-08. In reaching its decision the court relied upon United States v. Dowling, 473 U.S. 207 (1985). See also supra Section VI.B at page 93 (discussing application of Dowling to charging 18 U.S.C. § 2314 for intellectual property crimes).

The Brown court did distinguish a situation in which the defendant illegally appropriates a tangible item containing an intangible component, such as a chemical formula written on a stolen piece of paper. The court suggested that such an appropriation would violate 18 U.S.C. § 2314, even where the value of the paper itself is insignificant and the overall value is almost wholly derived from the intangible component. 925 F.2d at 1307-08 n.14 (citing United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988)).

The court in United States v. Bottone, 365 F.2d 389 (2d Cir.), cert. denied, 385 U.S. 974 (1966), which pre-dates Dowling, reached the opposite result. 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:

> 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 394. Similarly, in United States v. Riggs, 739 F. Supp. 414, 420 (N.D. Ill. 1990), the court rejected the 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." Id. at 421.[22]

Despite Brown, where the defendant has transported the intellectual property within a stolen tangible medium – for example, company paper or computer diskettes – courts have uniformly found that section 2314 or section 2315 applies. See United States v. Lyons, 992 F.2d 1029, 1033 (10th Cir. 1993) ("The fact that the [defendant] stole the 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.) (originals and copies of geophysical maps made by defendants on the victim's own copying equipment with the victim's supplies are covered under § 2314), cert. denied, 364 U.S. 937 (1961); United States v. Seagraves, 265 F.2d 876 (3d Cir. 1959) (same facts as Lester); United States v. Greenwald, 479 F.2d 320 (6th Cir.) (original documents containing trade secrets about fire retardation processes), cert. denied 414 U.S. 854 (1973); Hancock v. Decker, 379 F.2d 552 (5th Cir. 1967) (state conviction for theft of 59 copies of a computer program was supported by similar federal court rulings under § 2314, citing Seagraves).

[22] There are also at least two other decisions that, in general, support the position that transporting intangible property in interstate commerce violates 18 U.S.C. § 2314. However, both these cases involve the interstate transportation of illegal copies of copyrighted works and their continuing viability is suspect in light of the Supreme Court's decision in United States v. Dowling, which specifically held that 18 U.S.C. § 2314 does not reach the interstate transportation of unauthorized copies of copyrighted works. See United States v. Belmont, 715 F.2d 459 (9th Cir.) (holding that transporting in interstate commerce illegal "off the air" videotape copies of motion pictures protected by copyright violated 18 U.S.C. § 2314), cert. denied, 465 U.S. 1022 (1984); United States v. Gottesman, 724 F.2d 1517 (2d Cir. 1984) (holding among other things that intangible idea protected by copyright is effectively made tangible by its embodiment upon videotapes and thereby covered by the National Stolen Property Act) .

CONCLUSION

Intellectual property is an increasingly important part of the United States economy. Although misappropriation of intellectual property is on the rise, Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights. The current statutory scheme provides a workable means for law enforcement to investigate and prosecute intellectual property crimes. Among the most significant provisions are the following:

- The trademark counterfeiting crime is set out at 18 U.S.C. § 2320
- The infringement crime provisions at 17 U.S.C. § 506(a) and 18 U.S.C. § 2319
- The counterfeit labeling provision at 18 U.S.C. § 2318
- Theft of trade secrets is prohibited by 18 U.S.C. §§ 1831 & 1832

Experience has proven that federal investigators and prosecutors can bring cases under these provisions that result in punishment for the wrongdoer as well as deterrence for intellectual property crimes.

This manual is intended be a useful resource to law enforcement in investigating and prosecuting intellectual property crimes. In order for us to stay abreast of the current developments in this rapidly evolving area of the law, we would like to hear about prosecutions involving the criminal intellectual property statutes. Please also contact us with any comments, corrections or contributions regarding this manual or for legal advice or litigation assistance. We can be reached for such contact at (202) 514-1026.

APPENDIX A: Intellectual Property Contact List

1. Federal Law Enforcement Contacts

Organization	Address	Comments
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	Guidance and support on prosecuting intellectual property cases; resources and materials used for prosecuting intellectual property cases; active in development of intellectual property enforcement policy; support and oversight of the federal prosecution of intellectual property crimes and the Intellectual Property Rights Initiative Until October 11, 2001, coordination of approvals on prosecutions under 18 U.S.C. § 1832 of the Economic Espionage Act
Intellectual Property Rights Coordination Center, U.S. Customs Service & Federal Bureau of Investigation (FBI) (Joint center)	Intellectual Property Rights Coordination Center 1300 Pennsylvania Avenue NW Room 3.5A Washington, DC 20229 tel: 202-927-0810 fax: 202-927-4093	Joint center to coordinate enforcement of intellectual property rights by the U.S. Customs Service and the FBI

Organization	Address	Comments
Financial Crimes Section, Federal Bureau of Investigation (FBI), U.S. Department of Justice Participant in Intellectual Property Rights Coordination Center (see above)	J. Edgar Hoover FBI Building Financial Crimes Section 935 Pennsylvania Avenue NW Washington, DC 20535 http://www.fbi.gov tel: 202-324-6334 fax: 202-324-6248 email: ipr.fcs@fbi.gov	Support and oversight of the FBI's intellectual property rights enforcement program
U.S. Customs Service, U.S. Department of the Treasury Various groups: 1. Intellectual Property Rights Program 2. Intellectual Property Rights Branch, Office of Regulations and Rulings 3. CyberSmuggling Center Participant in Intellectual Property Rights Coordination Center (see above)	Intellectual Property Rights Program 1300 Pennsylvania Avenue NW Room 7.3A Washington, DC 20229 tel: 202-927-3944 fax: 202-927-1202 http://www.customs.treas.gov	Support and oversight of the U.S. Customs Service intellectual property rights enforcement program
	Intellectual Property Rights Branch Office of Regulations and Rulings U.S. Customs Service Washington, DC 20229 tel: 202-927-2330 fax: 202-927-1876	Guidance on questions relating to importation of infringing intellectual property
	CyberSmuggling Center Cyber Crimes Unit 1320 Random Hills Road Suite 400 Fairfax, VA 22030 tel: 703-293-8005 fax: 703-293-9127	Center to focus Customs resources on Internet crimes, including intellectual property rights violations (including music and software)

Organization	Address	Comments
Fraud Group, Postal Inspection Service, U.S. Postal Service	U.S. Postal Inspection Service Fraud Group 475 L'Enfant Plaza SW Washington, DC 20260-2169 tel: 202-268-5430 fax: 202-268-4563 http://www.framed.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.
Office of Criminal Investigations, Food and Drug Administration	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
National Fraud Center, Internet Fraud Complaint Center, FBI & National White Collar Crime Center (Joint center)	National Fraud Center / Internet Fraud Complaint Center http://www.ifccfbi.gov	Provides reporting of 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. Trademark Organization Contacts

Organization	Address	Comments
United States Patent and Trademark Office (USPTO)	General Information Services Division U.S. Patent and Trademark Office Crystal Plaza 3 Room 2C02 Arlington, VA 20231 tel: 800-786-9199 fax: 703-308-7048 To obtain a copy of a trademark registration: Office of Public Records Crystal Gateway 4 Suite 300 1213 Jefferson Davis Highway Arlington, VA 22202 tel: 800-972-6382 fax: 703-305-8759 http://www.uspto.gov	Information on obtaining certified copies of trademark registration
International Anti-Counterfeiting Coalition (IACC)	1725 K Street NW Suite 1101 Washington, DC 20036 tel: 202-223-6667 fax: 202-223-6668 http://www.iacc.org	Association representing industries affected by counterfeiting
International Trademark Association (INTA)	1133 Avenue of the Americas New York, NY 10036 tel: 212-768-9887 fax: 212-768-7796 http://www.inta.org	Association representing trademark owners in all industries

3. Copyright Organization Contacts

Organization	Address	Comments
Library of Congress	Copyright Office Certifications & Documents LM 402 Washington, DC 20559 tel: 202-707-6787 http://www.loc.gov/copyright	Information on obtaining certified copies of copyright registrations
American Film Marketing Association (AFMA)	10850 Wilshire Boulevard 9th Floor Los Angeles, CA 90024 tel: 310-446-1000 fax: 310-446-1600 http://www.afma.com	Association representing the independent motion picture and television industry
Association of American Publishers (AAP)	50 F Street NW Washington, DC 20001 tel: 202-347-3375 fax: 202-347-3690 http://www.publishers.org	Association representing 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)	1150 18th Street NW Suite 700 Washington, DC 20036 tel: 202-872-5500 fax: 202-872-5501 http://www.bsa.org	Association representing major software and e-commerce developers
Interactive Digital Software Association (IDSA)	1211 Connecticut Avenue NW Suite 600 Washington, DC 20036 tel: 202-223-2400 fax: 202-223-2401 http://www.idsa.com	Association representing companies that publish video and computer games for video consoles, personal computers and the Internet

Organization	Address	Comments
International Intellectual Property Alliance (IIPA)	1747 Pennsylvania Avenue NW Suite 825 Washington, DC 20006 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)	201 Massachusetts Avenue NE Suite C-3 Washington, DC 20002 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)	1255 23rd Street NW Suite 200 Washington, DC 20037 tel: 202-466-2396 fax: 202-466-2893 http://www.ipo.org	Association representing owners of intellectual property
Motion Picture Association of America (MPAA)	15503 Ventura Boulevard Encino, CA 91436 tel: 818-995-6600 fax: 818-382-1785 http://www.mpaa.org	Association representing the film and entertainment industry
Recording Industry Association of America (RIAA)	1330 Connecticut Avenue NW Suite 300 Washington, DC 20036 tel: 202-775-0101 fax: 202-775-7253 http://www.riaa.org	Association representing the United States recording industry
Software and Information Industry Association (SIIA)	1730 M Street NW Suite 700 Washington, DC 20036 tel: 202-452-1600 fax: 202-223-8756 http://www.siia.net	Association representing software and information industry

APPENDIX B: Sample Indictment and Jury Instructions for Trademark Counterfeiting, 18 U.S.C. § 2320

1. Sample Indictment for Trademark Counterfeiting

TRAFFICKING IN COUNTERFEIT GOODS OR SERVICES
18 U.S.C. § 2320

On or about the ___ day of _____, 2000, in the _____ District of _____, the defendant _____, did intentionally traffic in goods or services, specifically [describe items or services], knowingly using on or in connection with such goods or services a counterfeit mark, to wit a spurious mark identical to or substantially indistinguishable from [describe mark], which mark is in use and is registered for those goods or services on the principal register of the United States Patent and Trademark Office, the use of which counterfeit mark is likely to cause confusion, to cause mistake, and to deceive, in violation of Title 18 United States Code, Section 2320(a).

2. Sample Jury Instructions for Trademark Counterfeiting

TRAFFICKING IN COUNTERFEIT GOODS OR SERVICES
18 U.S.C. § 2320

Elements of the offense:

The defendant is charged in Count __ of the indictment with trafficking in counterfeit goods or services in violation of Section 2320(a) of Title 18 of the United States Code. In order for the defendant to be found guilty of this crime, the Government must prove each of the following elements beyond a reasonable doubt:

1. That the defendant trafficked or attempted to traffic in goods or services, specifically [describe items or services];

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

3. That the defendant used a counterfeit mark on or in connection with goods or services; and

4. That the defendant knew the mark so used was counterfeit.

Sources: 18 U.S.C. § 2320(a)

First element – trafficked in goods or services:

The first element is that the defendant trafficked or attempted to traffic in goods or services.

The term "traffic" means 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.

Sources: 18 U.S.C. §§ 2320(a) and (d)(2)

Second element – intentional:

The second element of the offense charged is that the trafficking or attempt to traffic was intentional.

An act is "intentional" if done deliberately or on purpose. The Government, however, is

not required to prove that the defendant intended to violate the law, only that the defendant acted deliberately or on purpose.

Sources: 18 U.S.C. § 2320(a)
United States v. Gantos, 817 F.2d 41, 42-43 (8th Cir.), cert. denied, 484 U.S. 860 (1987)
United States v. Baker, 807 F.2d 427, 428-30 (5th Cir. 1986)

Third element – use of counterfeit mark:

The third element is that the defendant used a counterfeit mark on or in connection with the goods or services.

A "counterfeit mark" is a mark that is spurious, or not genuine or authentic. It is identical with, or substantially indistinguishable from, a mark in use and registered for those same goods or services on the principal register in the United States Patent and Trademark Office. Finally, a counterfeit mark is a mark the use of which is likely to cause confusion, to cause mistake, or to deceive.

A certificate of registration from the United States Patent and Trademark Office is prima facie evidence of the validity of the registered mark, of the ownership of the mark, and of the owner's exclusive right to use the registered mark. That is, such a certificate is sufficient proof of the existence of a valid registered mark unless outweighed by other evidence in the case. The Government is not required to prove that the defendant knew the mark was so registered.

In determining whether there exists a likelihood of confusion, you may consider various factors, including the type of trademark, the similarity of the design, the similarity of the product, the identity of the retailers and purchasers, the similarity of the advertising media used, the defendant's intent, and any actual confusion. None of these factors, however, is essential to a finding of likely confusion.

The statute does not require a showing that the direct purchasers would be confused, mistaken or deceived. It is sufficient that there is a likelihood of confusion, mistake, or deception as to any member of the buying public, even a person who sees the product after its purchase. Therefore, it is not a defense that the defendant told the immediate purchaser that the item was not genuine. The test is whether an average consumer examining the product would be deceived into believing that the product was made by the genuine trademark owner.

Sources: 18 U.S.C. § 2320(a)
15 U.S.C. § 1057(b)
United States v. Hon, 904 F.2d 803, 806 (2nd Cir. 1990), cert. denied, 498 U.S. 1069 (1991)

United States v. Yamin, 868 F.2d 130, 133 (5th Cir.), cert. denied, 492 U.S. 924 (1989)
United States v. Gantos, 817 F.2d 41, 42-43 (8th Cir.), cert. denied, 484 U.S. 860 (1987)
United States v. Torkington, 812 F.2d 1347, 1352 (11th Cir. 1987)

Fourth element – knowledge:

The fourth and final element is that the defendant knew the mark so used was counterfeit. This means that the defendant was aware or had a firm belief of the counterfeit nature of the mark. This element may be satisfied through circumstantial evidence, such as the method of purchasing of the goods, the manner of delivery, packaging conventions, and an unusually low price.

[If you find beyond a reasonable doubt that the defendant deliberately closed his or her eyes to what would otherwise have been obvious and acted with a conscious purpose to avoid learning the truth that the mark was counterfeit, then you may conclude that the defendant knew the mark used was counterfeit. However, guilty knowledge may not be established by demonstrating that the defendant was merely negligent, foolish or mistaken. In addition, if you find that the defendant actually believed that the mark was genuine, he may not be convicted. It is entirely up to you whether you find that the defendant deliberately closed his or her eyes and any inference to be drawn from the evidence on this issue.][23]

Sources: 18 U.S.C. § 2320(a)
1 L. Sand, et. al., Modern Federal Jury Instructions 3A-1, 3A-2
United States v. Stewart, 185 F.2d 112, 126 (3rd Cir. 1999)
United States v. Sung, 51 F.2d 92, 94 (7th Cir. 1995)
Joint Statement on Trademark Counterfeiting Legislation, 130 Cong. Rec. H.121076, H.12076-77

---

[23] Care must be exercised when offering the so-called "conscious avoidance" or "ostrich" instruction in brackets above, first set forth in United States v. Jewell, 532 F.2d 697 (9th Cir.) (en banc), cert. denied, 426 U.S. 951 (1976). There are significant differences throughout the circuits regarding the appropriateness of such an instruction and the precise language to be used. Attorneys are well advised to consult local circuit opinion on this matter prior to proceeding with a Jewell instruction.

APPENDIX C: Sample Indictments and Jury Instructions for Criminal Copyright Infringement, 17 U.S.C. § 506(a) & 18 U.S.C. § 2319

1. Sample Indictment for Felony Copyright Infringement

CRIMINAL INFRINGEMENT OF A COPYRIGHT – FELONY
17 U.S.C. §506(a), 18 U.S.C. § 2319

On or about the ___ day of _____, 2000 [or a range of dates during a 180-day period], in the _____ District of _____, the defendant _____, did willfully {and for the purpose of commercial advantage or private financial gain} infringe the copyright of a copyrighted work, to wit [describe work, e.g., X Corporation Computer Program], by reproducing and distributing during a 180-day period ten (10) or more copies of the copyrighted work which have a retail value of $2,500 or more,[24] in violation of Title 17 United States Code, Section 506(a)(2) {506(a)(1)} and Title 18 United States Code, Section 2319(c)(1) {2319(b)(1)}.[25]

---

[24] A minority of circuits require that the Government affirmatively prove the absence of a "first sale" where the infringement is committed by distribution. See Section III.C.2 at page 50 (discussing the 'first sale' doctrine in criminal cases). In those circuits, it may be necessary to include language alleging the absence of a "first sale" in the indictment.

[25] In a felony copyright infringement case, there is a greater maximum penalty of 5 years (rather than 3 years) if the Government proves at trial that the infringement was for the purposes of commercial advantage or private financial gain. 18 U.S.C. §§ 2319(b)(1) and (c)(1). The additional requirement of proving the defendant acted for the purpose of commercial advantage or private financial gain is distinguished throughout this sample with fancy brackets ({…}).

2. Sample Jury Instructions for Felony Copyright Infringement

CRIMINAL INFRINGEMENT OF A COPYRIGHT – FELONY
17 U.S.C. § 506(a), 18 U.S.C. § 2319

Elements of the offense – felony copyright infringement:

The defendant is charged in Count __ of the indictment with the criminal infringement of a copyright in violation of Section 506(a)(2) {506(a)(1)} of Title 17 and Section 2319(c)(1) {2319(b)(1)} of Title 18 of the United States Code. In order for the defendant to be found guilty of this crime, the Government must prove each of the following elements beyond a reasonable doubt:

1. That a copyright exists for [describe work, e.g., X Corporation Computer Program];

2. That the defendants infringed the copyright in this software by reproducing or distributing copies of the copyrighted work;

3. That the defendant, in infringing the copyright, acted willfully; and

4. That the defendant reproduced or distributed during a 180-day period at least ten (10) copies of the software which have a total retail value of $2,500 or more.[26]

{5. That the act of infringement was for the purpose of commercial advantage or private financial gain.}[27]

Sources: 17 U.S.C. § 106
17 U.S.C. § 506(a)(2) {506(a)(1)}
18 U.S.C. § 2319(c)(1) {2319(b)(1)}

---

[26] A minority of circuits require that the Government affirmatively prove the absence of a "first sale" where the infringement is committed by distribution. See Section III.C.2 at page 50 (discussing the 'first sale' doctrine in criminal cases). In those circuits, it would be necessary to instruct the jury as to that additional element.

[27] In a felony copyright infringement case, there is a greater maximum penalty of 5 years (rather than 3 years) if the Government proves at trial that the infringement was for the purposes of commercial advantage or private financial gain. 18 U.S.C. §§ 2319(b)(1) and (c)(1). The additional requirement of proving the defendant acted for the purpose of commercial advantage or private financial gain is distinguished throughout this sample with fancy brackets ({…}).

First element – copyright exists:

The first element of this offense is that a copyright exists for [describe work].

A person who holds a copyright is entitled to a certificate of registration from the Copyright Office. This certificate is prima facie evidence of the validity of the copyright, meaning such evidence is sufficient to establish there is a valid copyright for the software unless outweighed by other evidence in the case.

Sources: 17 U.S.C. § 506
17 U.S.C. § 410(c)
United States v. Taxe, 540 F.2d 961, 966 (9th Cir. 1976), cert. denied, 429 U.S. 1040 (1977)
Autoskill v. National Educ. Support Sys., Inc., 994 F.2d 1476, 1487 (10th Cir. 1993)

Second element – infringement:

The second element of the offense is that the defendant infringed the copyright in this software by reproducing or distributing one or more copies of the software.

A "computer program" is a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.

A "copy" of a computer program is a material object in which a computer program is fixed by any method from which the computer program can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. The term includes the material object in which the work is first fixed.

An infringement of a copyright occurs whenever someone who is not the copyright owner and who has no authorization from the owner does an act that is the exclusive right of the copyright owner. Among the exclusive rights given to the owner of a valid copyright is the right to reproduce and the right to distribute the copyrighted work. In this case, the Government alleges that the defendant infringed the copyright by reproducing or distributing copies of the protected software.

The Government need not demonstrate that the alleged copies are identical to the original work in all respects. Infringement may be shown by demonstrating a "substantial similarity" between the original work and a copy. A copy is substantially similar to the original work if you find that an ordinary reasonable person would conclude the defendant unlawfully appropriated the copyright owner's work by taking material of substance and value.

You are further instructed that the Government may prove infringement through direct or circumstantial evidence.

Source: 17 U.S.C. §§ 101, 106(1) and (3)
18 U.S.C. § 2319(e)
Kepner-Tregoe, Inc., v. Leadership Software, Inc., 12 F.3d 527, 532 (5th Cir.), cert. denied, 513 U.S. 820 (1994)
McCulloch v. Albert E. Price, Inc., 823 F.2d 316, 318-19 (9th Cir. 1987)
United States v. Cross, 816 F.2d 297, 303 (7th Cir. 1987)
United States v. O'Reilly, 794 F.2d 613, 615 (11th Cir. 1986)
Atari, Inc. v. North American Philips Consumer Elec. Corp., 672 F.2d 607, 614 (7th Cir.), cert. denied, 459 U.S. 880 (1982)
Playboy Enterprises v. Frena, 839 F. Supp. 1552, 1556 (M.D. Fla. 1993)

Third element – willful intent:

The third element is that the defendant acted willfully when he or she infringed the copyright.

To act "willfully" means to act with knowledge that one's conduct is unlawful and with the intent to do something the law forbids, that is to say with the purpose to disobey or to disregard the law.

Whether the defendant acted willfully may be proven by the defendant's conduct and by all of the facts and circumstances surrounding the case. The Government may prove infringement through direct or circumstantial evidence.

Conduct is not "willful" if due to negligence, inadvertence, or mistake. Moreover, mere evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement.[28]

Sources: 17 U.S.C. § 506(a)
United States v. Cross, 816 F.2d 297, 300-1 (7th Cir. 1987)
1 L. Sand, et. al., Modern Federal Jury Instructions 3A-3

---

[28] Circuits differ whether to include a general instruction defining the term "willfully," with some rejecting a separate instruction because of the difficulty in formulating a single instruction that accurately encompasses the different meanings of this term. See 1A O'Malley et al., Federal Jury Practice and Instructions § 17.05 (5th ed. 2000). To the extent a general instruction defining "willfully" is recommended or approved, prosecutors should rely upon the appropriate pattern jury instruction approved in their circuit.

Fourth element – ten (10) copies with value of $2,500 or more within a 180-day period:

The fourth element of the offense is that the defendant reproduced or distributed at least ten (10) copies of the software with a total retail value of $2,500 or more within a 180-day period.

Sources: 17 U.S.C. § 506(a)(2)
18 U.S.C. § 2319(c)(1)

Optional enhancement:

{Fifth element – purpose of commercial advantage or private financial gain:

The fifth element is that the act of infringement was for the purpose of commercial advantage or private financial gain. The Government, however, need not prove that the defendant actually received a profit from the infringement. The Government need only establish that the defendant acted with the hope or expectation of some commercial advantage or private financial gain.}[29]

Sources: 17 U.S.C. § 506(a)(1)
18 U.S.C. § 2319(b)(1)
United States v. Cross, 816 F.2d 297, 300-1 (7th Cir. 1987)
United States v. Shabazz, 724 F.2d 1536, 1540 (11th Cir. 1984)}

[29] In a felony copyright infringement case, there is a greater maximum penalty of 5 years (rather than 3 years) if the Government proves at trial that the infringement was for the purposes of commercial advantage or private financial gain. 18 U.S.C. §§ 2319(b)(1) and (c)(1). The additional requirement of proving the defendant acted for the purpose of commercial advantage or private financial gain is distinguished throughout this sample with fancy brackets ({…}).

3. Sample Indictments for Misdemeanor Copyright Infringement

Note: Felony infringement requires proof that the defendant reproduced or distributed at least ten copies of the software with a total retail value of $2,500 or more within a 180-day period. In contrast, a misdemeanor offense may be established either by showing: (1) willful interference with any of the exclusive rights in copyrighted works for the purpose of commercial advantage or private financial gain; or (2) willful reproducing or distributing copyright works with a total retail value of at least $1,000 of the infringed items. 18 U.S.C. § 2319(b)(3), (c)(3). Both misdemeanor alternatives are provided here:

CRIMINAL INFRINGEMENT OF A COPYRIGHT – MISDEMEANOR
17 U.S.C. § 506(a), 18 U.S.C. § 2319

Misdemeanor copyright infringement – commercial advantage or private financial gain:

On or about the ___ day of _____, 2000, in the _____ District of _____, the defendant _____, did willfully and for the purpose of commercial advantage or private financial gain infringe the copyright of a copyrighted work, to wit [describe work, e.g., X Corporation Computer Program], by [describe nature of infringement], in violation of Title 17 United States Code, Section 506(a)(1) and Title 18 United States Code, Section 2319(b)(3).

Misdemeanor copyright infringement – total retail value of more than $1,000:

On or about the ___ day of _____, 2000, in the _____ District of _____, the defendant _____, did willfully infringe the copyright of a copyrighted work, to wit [describe work, e.g., X Corporation Computer Program], by reproducing and distributing within a 180-day period one or more copies of the copyrighted work which have a total retail value of more than $1,000, in violation of Title 17 United States Code, Section 506(a)(2) and Title 18 United States Code, Section 2319(c)(3).

4. Sample Jury Instructions for Misdemeanor Copyright Infringement

Note: Felony infringement requires proof that the defendant reproduced or distributed at least ten copies of the software with a total retail value of $2,500 or more within a 180-day period. In contrast, a misdemeanor offense may be established either by showing: (1) willful interference with any of the exclusive rights in copyrighted works for the purpose of commercial advantage or private financial gain; or (2) willful reproducing or distributing copyright works with a total retail value of at least $1,000 of the infringed items. 18 U.S.C. §§ 2319(b)(3) and (c)(3). Both misdemeanor alternatives are provided here with bracketed instructions to be given in cases of reproduction and distribution with a total retail value of $1,000 or more.

CRIMINAL INFRINGEMENT OF A COPYRIGHT – MISDEMEANOR
17 U.S.C. § 506(a), 18 U.S.C. § 2319

Elements of the offense – misdemeanor copyright infringement:

The defendant is charged in Count __ of the indictment with the criminal infringement of a copyright in violation of Section 506(a)(1) [or 506(a)(2)] of Title 17 and Section 2319(b)(3) [or 2319(c)(3)] of Title 18 of the United States Code. In order for the defendant to be found guilty of this crime, the Government must prove each of the following elements beyond a reasonable doubt:

1. That a copyright exists for [describe work, e.g., X Corporation Computer Program];

2. That the defendants infringed the copyright of this work by [describe nature of infringement] [or, if not for purposes of commercial advantage or private financial gain, "That the defendants infringed the copyright in this software by reproducing or distributing copies of the copyrighted work"];

3. That the defendant, in infringing the copyright, acted willfully; and

4. That the act of infringement was for the purpose of commercial advantage or private financial gain [or "That the defendant reproduced or distributed within a 180-day period one or more copies of the copyrighted work with a total retail value of more than $1,000"].

Sources: 17 U.S.C. § 506(a)(1) [506(a)(2)]
18 U.S.C. § 2319(b)(3) [2319(c)(3)]

Note: For jury instructions relating to the substance of these elements, see analogous

instructions from the felony copyright infringement instructions above.

APPENDIX D: Sample Indictment and Jury Instructions for Trafficking in Counterfeit Labels, 18 U.S.C. § 2318

1. Sample Indictments for Trafficking in Counterfeit Labels and Computer Program Documentation

Note: Federal law prohibits the trafficking in counterfeit labels affixed or designed to be affixed to certain copyrighted works, including a phonorecord, a copy of a computer program, a motion picture or other audiovisual work. 18 U.S.C. § 2318(a). In addition, the statute prohibits trafficking in counterfeit copyrighted documentation or packaging for a computer program. Id. Both alternatives are provided here:[30]

TRAFFICKING IN COUNTERFEIT LABELS
OR COMPUTER PROGRAM DOCUMENTATION
18 U.S.C. § 2318

Trafficking in counterfeit labels:

On or about the ___ day of _____, 2000, in the _____ District of _____, the defendant _____, did knowingly traffic in counterfeit labels affixed or designed to be affixed to [specify one of the following – a phonorecord, a copy of a computer program or documentation or packaging for a computer program, or a copy of a motion picture or other audiovisual work], to wit [describe item], a copyrighted work [or another circumstance establishing federal jurisdiction as set forth in 18 U.S.C. § 2318(c)], in violation of Title 18 United States Code, Sections 2318(a) and (c)(3) [or another subsection of § 2318(c) if not relying on copyright to establish federal jurisdiction].

---

[30] Federal jurisdiction is established most commonly by the copyright but the copyright is not necessary. Federal jurisdiction is provided by any of four circumstances: (1) the offense is committed within the special maritime and territorial jurisdiction of the United States or within the special aircraft jurisdiction of the United States; (2) the mail or a facility of interstate or foreign commerce is used or intended to be used in the commission of the offense; (3) the counterfeit label is affixed to or encloses or is designed to be affixed to or enclose, a copy of a copyrighted computer program, motion picture or other audiovisual work, or a phonorecord of a copyrighted sound recording; or (4) the counterfeited documentation or packaging for a computer program is itself copyrighted. 18 U.S.C. § 2318(c)(1)-(4).

Trafficking in counterfeit documentation or packaging for a computer program:

On or about the ___ day of _____, 2000, in the _____ District of _____, the defendant _____, did knowingly traffic in counterfeit copyrighted [or another circumstance establishing federal jurisdiction as set forth in 18 U.S.C. § 2318(c)] documentation or packaging for a computer program, to wit [describe documentation/packaging and computer program], in violation of Title 18 United States Code, Sections 2318(a) and (c)(4) [or another subsection of § 2318(c) if not relying on copyright to establish federal jurisdiction].

2. Sample Jury Instructions for Trafficking in Counterfeit Labels

TRAFFICKING IN COUNTERFEIT LABELS
18 U.S.C. § 2318

Elements of the Offense – trafficking in counterfeit labels:

The defendant is charged in Count ___ of the indictment with knowingly trafficking in counterfeit labels affixed or designed to be affixed to [specify one of the following – a phonorecord, a copy of a computer program or documentation or packaging for a computer program, or a copy of a motion picture or other audiovisual work], in violation of Section 2318(a) of Title 18 of the United States Code. In order for the defendant to be found guilty of this crime, the Government must prove each of the following elements beyond a reasonable doubt:

1. That the defendant acted knowingly;

2. That the defendant trafficked in counterfeit labels affixed or designed to be affixed to [specify one of the following – a phonorecord, a copy of a computer program or documentation or packaging for a computer program, or a copy of a motion picture or other audiovisual work], namely [describe item];

3. That the labels were counterfeit; and

4. That a copyright exists for [describe item] [or another circumstance establishing federal jurisdiction as set forth in 18 U.S.C. § 2318(c)].

Source: 18 U.S.C. §§ 2318(a) and (c)

First element (trafficking in counterfeit labels) – knowledge:

The first element the Government must prove is that the defendant acted knowingly. A person acts "knowingly" if he or she acts intentionally and voluntarily, and not because of ignorance, mistake, accident, or carelessness. Whether the defendant acted knowingly may be proven by the defendant's conduct and by all of the facts and circumstances surrounding the case.[31]

[In determining whether the defendant acted knowingly, you may consider whether the defendant deliberately closed his or her eyes to what would otherwise have been obvious to him.

---

[31] Prosecutors should rely upon the appropriate pattern jury instructions in their circuit to define "knowingly."

If you find beyond a reasonable doubt that the defendant acted with a conscious purpose to avoid learning the truth that the labels were counterfeit, then this element may be satisfied. However, guilty knowledge may not be established by demonstrating that the defendant was merely negligent, foolish or mistaken.

If you find that the defendant was aware of a high probability that the labels were counterfeit and that the defendant acted with deliberate disregard of the facts, you may find that the defendant acted knowingly. However, if you find that the defendant actually believed that the labels were not counterfeit, he may not be convicted.

It is entirely up to you whether you find that the defendant deliberately closed his or her eyes and any inference to be drawn from the evidence on this issue.][32]

Sources: 18 U.S.C. § 2318(a)
1 L. Sand, et. al., Modern Federal Jury Instructions 3A-1, 3A-2

Second element (trafficking in counterfeit labels) – trafficking in labels affixed or designed to be affixed to copies of a computer program:

The second element of the offense is that the defendant trafficked in labels affixed or designed to be affixed to copies of a computer program.

The term "traffic" means 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.

A "computer program" is a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.

A "copy" of a computer program is a material object in which a computer program is fixed by any method from which the computer program can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. The term includes the material object in which the work is first fixed.

The Government must prove that the labels were affixed or were designed to be affixed to

---

[32] Care must be exercised when offering the so-called "conscious avoidance" or "ostrich" instruction in brackets above, first set forth in United States v. Jewell, 532 F.2d 697 (9th Cir.) (en banc), cert. denied, 426 U.S. 951 (1976). There are significant differences throughout the circuits regarding the appropriateness of such an instruction and the precise language to be used. Attorneys are well advised to consult local circuit opinion on this matter prior to proceeding with a Jewell instruction.

a copy of a copyrighted computer program. The Government has proven this element if it establishes that the labels were affixed or designed to be so affixed, even if they had not yet been attached to the items in question.

Sources: 17 U.S.C. § 101
18 U.S.C. §§ 2318(a), (b)(2) and (b)(3)

Third element (trafficking in counterfeit labels) – labels were counterfeit:

The third element is that the labels that were counterfeit.

A "counterfeit label" is an identifying label or container that appears to be genuine, but is not.

Source: 18 U.S.C. § 2318(b)(1)

Fourth Element (trafficking in counterfeit labels) – work is copyrighted or another circumstance establishing federal jurisdiction pursuant to 18 U.S.C. § 2318(c):

[As noted above, federal jurisdiction is established in one of four circumstances. Described here is the situation of counterfeit labels affixed to a copyrighted work. 18 U.S.C. § 2318(c)(3).]

The fourth and final element of this offense is that a copyright exists for [describe item].

A person who holds a copyright is entitled to a certificate of registration from the Copyright Office. This certificate is prima facie evidence of the validity of the copyright, meaning such evidence is sufficient to establish there is a valid copyright for the software unless outweighed by other evidence in the case.

Sources: 18 U.S.C. § 2318(c)(3)
17 U.S.C. § 410(c)
United States v. Taxe, 540 F.2d 961, 966 (9th Cir. 1976), cert. denied, 429 U.S. 1040 (1977)
Autoskill v. National Educ. Support Sys., Inc., 994 F.2d 1476, 1487 (10th Cir. 1993)

3. Sample Jury Instructions for Trafficking in Counterfeit Documentation for a Computer Program

TRAFFICKING IN COUNTERFEIT DOCUMENTATION
FOR A COMPUTER PROGRAM
18 U.S.C. § 2318

Elements of the Offense – trafficking in counterfeit documentation:

The defendant is charged in Count ___ of the indictment with knowingly trafficking in counterfeit documentation or packaging for a computer program, in violation of Section 2318(a) of Title 18 of the United States Code. In order for the defendant to be found guilty of this crime, the Government must prove each of the following elements beyond a reasonable doubt:

1. That the defendant acted knowingly;

2. That the defendant trafficked in documentation or packaging for a computer program, namely [describe documentation/programming and computer program];

3. That the documentation or packaging were counterfeit; and

4. That a copyright exists for [describe documentation/packaging] [or another circumstance establishing federal jurisdiction as set forth in 18 U.S.C. § 2318(c)].

Source: 18 U.S.C. §§ 2318(a) and (c)

First element (trafficking in counterfeit documentation) – knowledge:

[See analogous instructions from the counterfeit label trafficking example above.]

Second element (trafficking in counterfeit documentation) – trafficking in documentation or packaging:

The second element of the offense is that the defendant trafficked in documentation or packaging for a computer program.

The term "traffic" means 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.

A "computer program" is a set of statements or instructions to be used directly or

indirectly in a computer in order to bring about a certain result.

Sources: 17 U.S.C. § 101
18 U.S.C. §§ 2318(a), (b)(2) and (b)(3)

Third element (trafficking in counterfeit documentation) – documentation or packaging were counterfeit:

The third element is that the documentation or packaging that were counterfeit.

Counterfeit packaging or documentation is packaging or documentation that appears to be genuine, but is not.

Source: 18 U.S.C. § 2318(b)(1)

Fourth Element (trafficking in counterfeit packaging) – documentation/packaging is copyrighted or another circumstance establishing federal jurisdiction pursuant to 18 U.S.C. § 2318(c):

[As noted above, federal jurisdiction is established in one of four circumstances. Described here is the situation of counterfeit documentation or packaging that is itself copyrighted. 18 U.S.C. § 2318(c)(4).]

The fourth and final element of this offense is that the counterfeited documentation or packaging for a computer program is copyrighted.

A person who holds a copyright is entitled to a certificate of registration from the Copyright Office. This certificate is prima facie evidence of the validity of the copyright, meaning such evidence is sufficient to establish there is a valid copyright for the software unless outweighed by other evidence in the case.

Sources: 18 U.S.C. § 2318(c)(4)
17 U.S.C. § 410(c)
United States v. Taxe, 540 F.2d 961, 966 (9th Cir. 1976), cert. denied, 429 U.S. 1040 (1977)
Autoskill v. National Educ. Support Sys., Inc., 994 F.2d 1476, 1487 (10th Cir. 1993)

APPENDIX E: Sample Indictment and Jury Instructions for the Theft of Trade Secrets, 18 U.S.C. § 1832

1. Sample Indictment for the Theft of Trade Secrets

THEFT OF TRADE SECRETS
18 U.S.C. § 1832

On or about the ___ day of _____, 2000, in the _____ District of _____, the defendant _____, did knowingly steal and appropriate without authorization a trade secret, specifically [describe item or information misappropriated], related to or included in a product that is produced for or placed in interstate or foreign commerce, intending that the theft would economically benefit someone other than the owner thereof, and intending or knowing that the offense would injure the owner of the trade secret, in violation of Title 18, United States Code, Section 1831(b)(1).[33]

[33] Theft of trade secrets includes not only misappropriation but also the duplication, transmission, destruction, receipt, purchase or possession of trade secrets, as well as conspiracy or attempt to commit any of the above. 18 U.S.C. § 1832(b)(1)-(5). This sample addresses only the misappropriation of trade secrets as set forth in § 1832(b)(1).

2. Sample Jury Instructions for the Theft of Trade Secrets

THEFT OF TRADE SECRETS
18 U.S.C. § 1832

Elements of the offense:

The defendant is charged in Count ___ of the indictment with theft of trade secrets, in violation of Section 1832(b) of Title 18 of the United States Code. In order for the defendant to be found guilty of this crime, the Government must prove each of the following elements beyond a reasonable doubt:

1. That the defendant stole or appropriated without authorization from the owner [describe the item or information misappropriated];

2. That the defendant knew or had a firm belief that the [item/information] was a trade secret;

3. That the [item/information] was in fact a trade secret;[34]

4. That the defendant intended to convert the trade secret to the economic benefit of anyone other than the owner;

5. That the defendant intended or knew the theft would injure the owner of the trade secret; and

6. That the trade secret was related to or was included in a product that was produced for or placed in interstate or foreign commerce.

Source: 18 U.S.C. § 1832

First element – theft or misappropriation:

The first element of the offense is misappropriation. The Government must prove that the defendant stole or without authorization from the owner appropriated, took, carried away, or concealed, or by fraud, artifice, or deception obtained the [item/information]. To act without authorization is to act without the permission, approval, consent or sanction of the owner.

---

[34] When the charge is attempt or conspiracy, the Government need not prove the existence of a trade secret. United States v. Hsu, 155 F.3d 189, 198 (3d Cir. 1998) (crimes of attempt and conspiracy "do not require proof of the existence of an actual trade secret, but, rather, proof only of one's attempt or conspiracy with intent to steal a trade secret").

The term "owner" means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.

Source: 18 U.S.C. §§ 1832(b)(1), 1839(4)

Second element – knowledge:

The second element of the offense is whether the defendant knew or had a firm belief that the information taken was a trade secret. Whether the defendant was aware or had a firm belief that the information was a trade secret may be proven by the defendant's conduct and by all of the facts and circumstances surrounding the case, including but not limited to evidence of proprietary markings, security measures and confidentiality agreements. It is entirely up to you what inferences, if any, are to be drawn from the evidence on this issue.

However, if you find that the defendant actually believed that the information was not a trade secret, or if you conclude the defendant obtained the information because of ignorance, mistake or accident, then the defendant may not be convicted of this offense.

Sources: 18 U.S.C. § 1832(a)
142 Cong. Rec. S12202, S12213 (daily ed. Oct. 2, 1996)

Third element – existence of a trade secret:

The third element is that the [item/information] was in fact a trade secret. You are instructed that a "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.

The Government must establish that the owner of the information took reasonable measures to keep such information secret. These security measures need not be absolute, but reasonable under the circumstances.

In addition, the Government must prove that the information was not generally known to the public, or could not be reasonably ascertained through proper means by the public. However, not every part of the information must be confidential to constitute a trade secret. A trade secret can include a combination of elements that are in the public domain if the trade secret constituted a unique, effective, successful and valuable integration of public domain elements.

Finally, the Government must establish that the information derives independent

economic value, whether actual or potential, from not being generally known to the public. However, the Government is not required to prove with precision the value of the trade secret, only that there is some independent value to the information on its status as a trade secret. You may consider the open market value of the [item/information], development, research and production costs, and the "black market" price the [item/information] would fetch.

Sources: 18 U.S.C. § 1839(3)
Reingold v. Swiftships, Inc., 126 F.3d 645, 650 (5th Cir. 1997)
Buffets, Inc. v. Klinke, 73 F.3d 965, 968 (9th Cir. 1996)
Pioneer Hi-Bred Int'l v. Holden Found. Seeds, 35 F.3d 1226, 1235 (8th Cir. 1994)
Rivendell Forest Prods., Ltd. v. Georgia-Pacific Corp., 28 F.3d 1042, 1046 (10th Cir. 1994)
Gates Rubber Co. v. Bando Chem. Indus., Ltd., 9 F.3d 823, 828-49 (10th Cir. 1993)
United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988)

Fourth element – economic benefit:

The fourth element of the offense is that the defendant intended to convert the trade secret to the economic benefit of anyone other than the owner. The Government need not prove that the defendant himself profited by the theft. Rather, the Government has the burden of proving that the defendant intended that a person or business other than the rightful owner of the trade secret benefitted economically from the misappropriation.

Source: 18 U.S.C. § 1832(a)

Fifth element – injury to the owner:

The fifth element is that the defendant intended or knew the theft would injure the owner of the trade secret. The Government is not required to prove malice or evil intent, but that the defendant knew or was aware to a practical certainty that his conduct would cause some disadvantage to the rightful owner.

Source: 18 U.S.C. § 1832(a)
H.R. Rep. No. 788, 104th Cong., 2d Sess. 1996.

Sixth element – interstate or foreign commerce:

The sixth and final element is that the trade secret was related to or included in a product that was produced for or placed in interstate or foreign commerce. If you find that the trade

secret was part of a product, in any stage of production, including research, development and manufacture, and was produced for or placed in interstate or foreign commerce, you may conclude that the Government has proven this element.

Source: 18 U.S.C. § 1832(a)

APPENDIX F: Relevant State Statutes

1. State Criminal Trademark Infringement Statutes

1.	Alabama	Ala. Code § 13A-8-10.4 (1994) (Felony)
2.	Alaska	No statute; forgery statute includes Alaska Stat. § 11.46.510 (Michie 1998) (Misdemeanor)
3.	Arizona	Ariz. Rev. Stat. Ann. §§ 44-1453, -1456 (West 1994 & Supp. 1999) (Felony and Misdemeanor, depends on violation)
4.	Arkansas	No statute.
5.	California	Cal. Penal Code § 350 (West 1999 & Supp. 2000) (Felony and Misdemeanor, depends on quantity)
6.	Colorado	Colo. Rev. Stat. Ann. § 7-73-108 (West 1999) (Misdemeanor)
7.	Connecticut	Conn. Gen. Stat. § 53-347a (1999) (Felony)
8.	Delaware	No statute; forgery statute includes Del. Code Ann. tit. 11, § 861 (1995 & Supp. 1998) (Felony and Misdemeanor, depends on type)
9.	District of Columbia	D.C. Code Ann. §§ 22-751 to -752, -1402 (1981 & Supp. 1991) (Felony and Misdemeanor, depends on quantity)
10.	Florida	Fla. Stat. Ann. §§ 831.03, .05 (West 1994 & Supp. 2000) (Felony and Misdemeanor, depends on value)
11.	Georgia	Ga. Code Ann. § 10-1-454 (Harrison 1998) (Felony)
12.	Hawaii	Haw. Rev. Stat. Ann. § 708-875 (Michie 1999) (Felony)
13.	Idaho	No statute; forgery statute includes Idaho Code §§ 18-3601, -3604 (1997) (Felony)
14.	Illinois	765 Ill. Comp. Stat Ann. 1040/1-1040/2 (West 1993 & Supp. 1999) (Felony and Misdemeanor, depends on violation)
15.	Indiana	No statute; forgery statutes include Ind. Code Ann. §§ 35-43-5-1 to -2 (Michie 1998) (Felony)
16.	Iowa	No statute; counterfeit statute includes Iowa Code Ann. § 714.8 (West 1993 & Supp. 2000) (Misdemeanor)
17.	Kansas	No statute; forgery statutes include Kan. Stat. Ann. §§ 21-3110, -3710 (1995) (Felony)
18.	Kentucky	No statute; forgery statutes include Ky. Rev. Stat. Ann. §§ 516.040, .070 (Michie 1999) (Misdemeanor)
19.	Louisiana	La. Rev. Stat. Ann. § 14:229 (West 1986) (Felony)
20.	Maine	No statute; forgery statutes include Me. Rev. Stat. Ann. tit. 17-A,§§ 703-705 (West 1983 & Supp. 1999) (Felony)
21.	Maryland	Md. Ann. Code art. 27, § 48A (1996) (Felony and Misdemeanor, depends on value)
22.	Massachusetts	Mass. Gen. Laws Ann. ch. 266, § 147 (West 1999) (Felony)
23.	Michigan	Mich. Comp. Laws Ann. §§ 750.263-.264 (West 1999 & Supp. 1999) (Felony and Misdemeanor, depends on violation)
24.	Minnesota	Minn. Stat. Ann. § 609.895 (West Supp. 2000) (Felony)

25.	Mississippi	Miss. Code Ann. §§ 97-21-53 to -57 (1999) (Felony)
26.	Missouri	No statute; forgery and counterfeit statutes include Mo. Ann. Stat. §§ 570.090-.105 (West 1999 & Supp. 2000) (Felony)
27.	Montana	No statute; forgery statute includes Mont. Code Ann. § 45-6-325 (1999) (Felony and Misdemeanor, depends on value)
28.	Nebraska	No statute; forgery statute includes Neb. Rev. Stat. § 28-603 (1995) (Felony and Misdemeanor, depends on value)
29.	Nevada	Nev. Rev. Stat. Ann. §§ 205.205-.210 (Michie 1997 & Supp. 1999); Nev. Rev. Stat. Ann. § 600.450 (Michie 1999) (Misdemeanor)
30.	New Hampshire	No statute; forgery statute includes N.H. Rev. Stat. Ann. § 638.1 (1996) (Misdemeanor)
31.	New Jersey	1999 N.J. Sess. Law. Serv. 313 (West) (Felony)
32.	New Mexico	No statute; forgery statute includes N.M. Stat. Ann. § 30-16-10 (Michie 1994 & Supp. 1999) (Felony)
33.	New York	N.Y. Penal Law §§ 165.70-.74 (McKinney 1999 & Supp. 1999-2000) (Felony and Misdemeanor, depends on situation)
34.	North Carolina	N.C. Gen. Stat. §§ 80-11 to -11.1 (1999) (Felony and Misdemeanor, depends on value)
35.	North Dakota	No statute; forgery statutes include N.D. Cent. Code §§ 12.1-24-01, -04 (1997) (Felony)
36.	Ohio	Ohio Rev. Code Ann. § 2913.34 (Anderson 1996) (Felony)
37.	Oklahoma	Okla. Stat. Ann. tit. 21, §§ 1990.1-.2 (West Supp. 2000) (Felony and Misdemeanor, depends on violation)
38.	Oregon	1999 Or. Laws 722. (Felony)
39.	Pennsylvania	18 Pa. Cons. Stat. Ann. § 4119 (West Supp. 1999) (Felony and Misdemeanor, depends on quantity)
40.	Rhode Island	R.I. Gen. Laws § 11-17-13 (Supp. 1999) (Felony and Misdemeanor, depends on value)
41.	South Carolina	S.C. Code Ann. § 39-15-1190 (Law Co-op. Supp. 1997) (Misdemeanor)
42.	South Dakota	S.D. Codified Laws §§ 37-6-1 to -3 (Michie 1994) (Misdemeanor)
43.	Tennessee	Tenn. Code Ann. § 47-25-513 (1995) (Misdemeanor)
44.	Texas	Tex. Penal Code Ann. § 32.23 (West Supp. 2000) (Felony and Misdemeanor, depends on value)
45.	Utah	Utah Code Ann. §§ 76-10-1001 to -1007 (1999) (Misdemeanor)
46.	Vermont	Vt. Stat. Ann. tit. 9, § 2530 (1993) (Misdemeanor)
47.	Virginia	Va. Code Ann. § 59.1-92.12 (Michie 1998) (Felony, 1st offense Misdemeanor)
48.	Washington	Wa. Rev. Code Ann. §§ 9.16.005, .030-.035, .041 (West 1998 & Supp. 2000) (Felony and Misdemeanor, depends on violation)
49.	West Virginia	W. Va. Code § 47-2-12 (1999) (Misdemeanor)
50.	Wisconsin	Wis. Stat. Ann. §§ 132.02, .19, .20 (West 1989 & Supp. 1999)

		(Misdemeanor)
51.	Wyoming	No statute; forgery statutes include Wyo. Stat. Ann. §§ 6-3-601 to -603 (Michie 1999) (Felony and Misdemeanor, depends on violation)
52.	Puerto Rico	P.R. Laws Ann. tit. 33, §§ 1311-1316 (1983 & Supp)(Misdemeanor)

2. State Statutes Mandating Disclosure of Manufacturer's True Name and Address

1.	Alabama	Ala. Code § 13A-8-83 (1994) (Felony)
2.	Alaska	Alaska Stat. § 45.50.900(a)(2) (Michie 1998) (Misdemeanor)
3.	Arizona	Ariz. Rev. Stat. Ann. § 13-3705(A)(3)-(4) (West 1989 & Supp. 1998) (Felony and Misdemeanor, depends on quantity)
4.	Arkansas	Ark. Code Ann. § 5-37-510(c) (Michie 1997) (Felony and Misdemeanor, depends on quantity)
5.	California	Cal. Penal Code § 653w (West 1999) (Felony)
6.	Colorado	Colo. Rev. Stat. Ann. § 18-4-604 (West 1999) (Misdemeanor)
7.	Connecticut	Conn. Gen. Stat. Ann. § 53-142c, -142f (West 1997) (Misdemeanor)
8.	Delaware	Del. Code Ann. tit. 11, § 922 (1995) (Misdemeanor)
9.	District of Columbia	D.C. Code Ann. § 22-3814.1 (1996) (Felony and Misdemeanor, depends on quantity)
10.	Florida	Fla. Stat. Ann. § 540.11(3)(a)(3) (West 1997) (Felony)
11.	Georgia	Ga. Code Ann. § 16-8-60(b) (Harrison 1998) (Felony)
12.	Hawaii	No statute
13.	Idaho	Idaho Code § 18-7603(3) (1997) (Misdemeanor)
14.	Illinois	720 Ill. Comp. Stat. Ann. 5/16-8 (West 1993) (Felony)
15.	Indiana	Ind. Code Ann. §§ 24-4-10-1 to -5 (Michie 1996); Ind. Code Ann. § 35-43-5-4 (11) (Michie 1998) (Felony)
16.	Iowa	Iowa Code Ann. § 714.15(2) (West 1993) (Felony)
17.	Kansas	Kan. Stat. Ann. § 21-3750 (1996) (Felony and Misdemeanor, depends on quantity)
18.	Kentucky	Ky. Rev. Stat. Ann. § 434.445(4) (Michie 1985 & Supp. 1998) (Felony)
19.	Louisiana	La. Rev. Stat. Ann. §§ 14:223.6-.7 (West 1998 & Supp. 1999) (Felony and Misdemeanor, depends on quantity)
20.	Maine	No statute
21.	Maryland	Md. Ann. Code art. 27, § 467A(b) (1996) (Felony, Misdemeanor 1st offense)
22.	Massachusetts	Mass. Gen. Laws Ann. ch. 266, §143C (West 1992) (Felony)
23.	Michigan	Mich. Comp. Laws Ann. §§ 752.1052(1)(d), 752.1053 (Felony and Misdemeanor, depends on quantity)
24.	Minnesota	Minn. Stat. Ann. § 325E.18 (West 1995) (Felony)
25.	Mississippi	Miss. Code Ann. § 97-23-89 (1999) (Felony)
26.	Missouri	Mo. Ann. Stat. §§ 570.240-.241 (West 1999) (Felony, Misdemeanor 1st offense)
27.	Montana	Mont. Code Ann. § 30-13-144 (1997) (Misdemeanor)
28.	Nebraska	Neb. Rev. Stat. Ann. § 28-1324 (Michie 1995) (Misdemeanor)
29.	Nevada	Nev. Rev. Stat. Ann. § 205.217(2) (Michie 1997) (Felony)

30.	New Hampshire	N.H. Rev. Stat. Ann. § 352-A:3 (1995) (Violation)
31.	New Jersey	N.J. Stat. Ann. § 2C:21-21(c)(4) (West 1995) (Felony)
32.	New Mexico	N.M. Stat. Ann. § 30-16B-4 (Michie 1994) (Felony and Misdemeanor, depends on quantity)
33.	New York	N.Y. Penal Law §§ 275.35-.40 (McKinney 1999) (Felony and Misdemeanor, depend on violation)
34.	North Carolina	N.C. Gen. Stat. § 14-435 (1993) (Felony)
35.	North Dakota	N.D. Cent. Code § 47-21.1-03 (1978) (Misdemeanor)
36.	Ohio	Ohio Rev. Code Ann. §§ 1333.52(B), 1333.99(F) (Anderson 1993 & Supp. 1998) (Misdemeanor)
37.	Oklahoma	Okla. Stat. Ann. tit. 21, §§ 1979-1980 (West Supp. 1997) (Felony and Misdemeanor, depends on quantity)
38.	Oregon	Or. Rev. Stat. § 164.868 (1990 & Supp. 1998) (Felony)
39.	Pennsylvania	18 Pa. Cons. Stat. Ann. § 4116(e) (West 1983 & Supp. 1998) (Felony, 1st offense Misdemeanor)
40.	Rhode Island	R.I. Gen. Laws § 6-13.1-15(b) (1992) (Felony)
41.	South Carolina	S.C. Code Ann. §§ 16-11-930 to -940 (Law Co-op. 1985 & Supp. 1997) (Felony and Misdemeanor, depends on violation)
42.	South Dakota	S.D. Codified Laws § 43-43A-3 (Michie 1997) (Felony)
43.	Tennessee	Tenn. Code Ann. §§ 39-14-115(a)(1), 39-14-139(a) (1997) (Felony and Misdemeanor, depends on value)
44.	Texas	Tex. Bus. & Com. Code Ann. § 35.94 (West Supp. 1998) (Felony and Misdemeanor, depends on violation)
45.	Utah	Utah Code Ann. § 13-10-8 (1996) (Felony and Misdemeanor, depends on quantity)
46.	Vermont	No Statute
47.	Virginia	Va. Code Ann. § 59.1-41.3 to .4 (Michie 1998) (Felony and Misdemeanor, depends on quantity)
48.	Washington	Wa. Rev. Code Ann. § 19.25.040 (West 1999) (Felony)
49.	West Virginia	W. Va. Code § 61-3-50(a) (1997) (Felony)
50.	Wisconsin	Wis. Stat. Ann. § 943.209 (West Supp. 2000) (Felony and Misdemeanor, depends on quantity)
51.	Wyoming	No statute
52.	Puerto Rico	P.R. Laws Ann. tit. 33, § 2170(c) (Supp. 1995-1996) (Felony)

3. State Anti-bootlegging Statutes

1.	Alabama	Ala. Code § 13A-8-81(a)(2) (1994) (Felony)
2.	Alaska	No statute
3.	Arizona	Ariz. Rev. Stat. Ann. § 13-3705(A)(5) (West 1989 & Supp. 1998) (Felony)
4.	Arkansas	Ark. Code Ann. § 5-37-510(b) (Michie 1997) (Felony and Misdemeanor, depends on quantity)
5.	California	Cal. Penal Code §§ 653s, 653u (West 1999) (Felony)
6.	Colorado	No statute
7.	Connecticut	No statute
8.	Delaware	No statute
9.	DC	D.C. Code Ann. § 22-3814(b) (1996) (Misdemeanor)
10.	Florida	Fla. Stat. Ann. § 540.11(2)(a)(3), (3)(a)(2) (West 1997) (Felony)
11.	Georgia	No statute
12.	Hawaii	No statute
13.	Idaho	No statute
14.	Illinois	720 Ill. Comp. Stat. Ann. 5/16-7(a)(4) (West 1993) (Felony)
15.	Indiana	Ind. Code Ann. § 35-43-4-1(b)(8)(B) (Michie 1998) (Felony)
16.	Iowa	No statute
17.	Kansas	Kan. Stat. Ann. §§ 21-3748(a), 21-3749 (West 1996) (Felony)
18.	Kentucky	Ky. Rev. Stat. Ann. § 434.445(2) (Michie 1985 & Supp. 1998) (Felony)
19.	Louisiana	La. Rev. Stat. Ann. § 14:223.5 (West 1998) (Felony and Misdemeanor, depends on quantity)
20.	Maine	No statute
21.	Maryland	Md. Ann. Code art. 27, § 467A(a)(2)-(3) (1996) (Felony, 1st offense Misdemeanor)
22.	Massachusetts	Mass. Gen. Laws Ann. ch. 266, §143B (West 1992) (Felony)
23.	Michigan	Mich. Comp. Laws Ann. § 752.1052(1)(a) (West Supp. 1999) (Felony and Misdemeanor, depends on quantity)
24.	Minnesota	No statute
25.	Mississippi	Miss. Code Ann. § 97-23-87(2)(b) (1999) (Felony)
26.	Missouri	Mo. Ann. Stat. §§ 570.226-230 (West 1999) (Felony, 1st offense Misdemeanor)
27.	Montana	Mont. Code Ann. §§ 30-13-142(2), 30-13-143(2) (1997) (Felony)
28.	Nebraska	No statute
29.	Nevada	No statute
30.	New Hampshire	N.H. Rev. Stat. Ann. § 352-A:2(I)(b)(Felony), (II)(b)(Misdemeanor)(1995 & Supp. 1998).
31.	New Jersey	N.J. Stat. Ann. § 2C:21-21(c)(3) (West 1995) (Felony)
32.	New Mexico	N.M. Stat. Ann. § 30-16B-5 (Michie 1998) (Felony and Misdemeanor, depends on amount)

33.	New York	N.Y. Penal Law §§ 275.15-.20 (McKinney 1999) (Felony and Misdemeanor, depends on violation)
34.	North Carolina	N.C. Gen. Stat. § 14-433(a)(3)-(4) (1993) (Felony and Misdemeanor, depends on quantity)
35.	North Dakota	N.D. Cent. Code § 47-21.1-02(2)(felony)-(4)(misdemeanor) (1978) (Felony)
36.	Ohio	No statute
37.	Oklahoma	Okla. Stat. Ann. tit. 21, § 1978 (West Supp. 1997) (Felony and Misdemeanor, depends on quantity)
38.	Oregon	Or. Rev. Stat. § 164.869 (1990 & Supp. 1998) (Felony)
39.	Pennsylvania	18 Pa. Cons. Stat. Ann. § 4116(d.1) (West 1983 & Supp. 1998) (Felony)
40.	Rhode Island	R.I. Gen. Laws § 6-13.1-15(a)(2)-(3) (1992) (Felony)
41.	South Carolina	S.C. Code Ann. § 16-11-915 (Law Co-op. 1985 & Supp. 1997) (Felony and Misdemeanor, depends on violation)
42.	South Dakota	No statute
43.	Tennessee	Tenn. Code Ann. § 39-14-139(c) (1997) (Felony and Misdemeanor, depends on value)
44.	Texas	Tex. Bus. & Com. Code Ann. § 35.93 (West Supp. 1998) (Felony and Misdemeanor, depends on violation)
45.	Utah	No statute
46.	Vermont	No statute
47.	Virginia	Va. Code Ann. § 59.1-41.2 (Michie 1998) (Felony and Misdemeanor, depends on quantity)
48.	Washington	Wa. Rev. Code Ann. § 19.25.030 (1999) (Felony)
49.	West Virginia	W. Va. Code § 61-3-50(a) (1997) (Felony)
50.	Wisconsin	Wis. Stat. Ann. § 943.208 (West Supp. 2000) (Felony and Misdemeanor, depends on quantity)
51.	Wyoming	Wyo. Stat. Ann. § 40-13-202(a)(ii) (Michie 1999) (Felony)
52.	Puerto Rico	P.R. Laws Ann. tit. 33, §§ 2168-2171 (Supp. 1995-1996) (Felony)

4. State Piracy or Unauthorized Duplication Statutes

1.	Alabama	Ala. Code §§ 13A-8-81 to -82 (1994) (Felony)
2.	Alaska	Alaska Stat. § 45.50.900(a) (Michie 1998) (Misdemeanor)
3.	Arizona	Ariz. Rev. Stat. Ann. § 13-3705(A) (West 1989 & Supp. 1998) (Felony)
4.	Arkansas	Ark. Code Ann. § 5-37-510(b) (Michie 1997) (Felony)
5.	California	Cal. Penal Code § 653h (West 1999) (Felony)
6.	Colorado	Colo. Rev. Stat. Ann. §§ 18-4-602 to -603 (West 1999) (Felony)
7.	Connecticut	Conn. Gen. Stat. Ann. §§ 53-142b (Misdemeanor) , -142f (Felony) (West 1997).
8.	Delaware	Del. Code Ann. tit. 11, §§ 920-921 (1995) (Felony)
9.	DC	D.C. Code Ann. § 22-3814 (1996) (Misdemeanor)
10.	Florida	Fla. Stat. Ann. § 540.11(2)(a)(1)-(2) (West 1997) (Felony)
11.	Georgia	Ga. Code Ann. § 16-8-60(a) (Harrison 1998) (Felony)
12.	Hawaii	Haw. Rev. Stat. Ann. §§ 482C-1 to -2 (Michie 1998) (Misdemeanor)
13.	Idaho	Idaho Code § 18-7603(1)-(2) (1997) (Felony)
14.	Illinois	720 Ill. Comp. Stat. Ann. 5/16-7(a)(1)-(2), -8(a) (West 1993) (Felony)
15.	Indiana	No statute; theft and forgery statutes include Ind. Code Ann. §§ 35-43-4-2,35-43-5-2(4) (Michie 1998) (Felony)
16.	Iowa	Iowa Code Ann. § 714.15(1) (West 1993) (Felony)
17.	Kansas	Kan. Stat. Ann. §§ 21-3748 to -3749 (1996) (Felony)
18.	Kentucky	Ky. Rev. Stat. Ann. § 434.445(1), (3) (Michie 1985 & Supp. 1998) (Felony)
19.	Louisiana	La. Rev. Stat. Ann. § 14:223 (West 1998 & Supp. 1999) (Felony)
20.	Maine	Me. Rev. Stat. Ann. tit.10, § 1261(1)-(2) (West 1997) (Fine)
21.	Maryland	Md. Ann. Code art. 27, § 467A(a) (1996). (Felony, 1st offense Misdemeanor)
22.	Massachusetts	Mass. Gen. Laws Ann. ch. 266, § 143A (West 1992) (Felony)
23.	Michigan	Mich. Comp. Laws Ann. § 752.1052(b)-(c) (West Supp. 1999) (Felony and Misdemeanor, depends on quantity)
24.	Minnesota	Minn. Stat. Ann. § 325E.17 (West 1995) (Felony)
25.	Mississippi	Miss. Code Ann. § 97-23-87(2)(a), (3)(a)(i), (3)(a)(iii) (1999) (Felony)
26.	Missouri	Mo. Ann. Stat. §§ 570.225-.230, -.255 (West 1999) (Felony, 1st offense Misdemeanor)
27.	Montana	Mont. Code Ann. §§ 30-13-142(1), (3), -143(1), (3) (1997) (Felony)
28.	Nebraska	Neb. Rev. Stat. Ann. §§ 28-1323 (Michie 1995) (Misdemeanor)
29.	Nevada	Nev. Rev. Stat. Ann. § 205.217(1) (Michie 1997) (Felony)
30.	New Hampshire	N.H. Rev. Stat. Ann. § 352-A:2(I)(a)(Felony), (II)(a) (Misdemeanor) (1995 & Supp. 1998)
31.	New Jersey	N.J. Stat. Ann. § 2C:21-21(c)(1)-(2), (d) (West 1995) (Felony)
32.	New Mexico	N.M. Stat. Ann. § 30-16B-3(A) (Michie 1994) (Felony and Misdemeanor, depends on quantity)

33.	New York	N.Y. Penal Law §§ 275.05-.10, 275.25-.30 (McKinney 1999) (Felony)
34.	North Carolina	N.C. Gen. Stat. §§ 14-433(a), -434 (1993) (Felony and Misdemeanor, depends on quantity)
35.	North Dakota	N.D. Cent. Code § 47-21.1-02(1) (Felony), (3) (1978) (Misdemeanor).
36.	Ohio	Ohio Rev. Code Ann. § 1333.52(A) (Misdemeanor) (Anderson 1993 & Supp. 1998); Ohio Rev. Code Ann. § 2913.32(A)(2) (Anderson 1996) (Felony)
37.	Oklahoma	Okla. Stat. Ann. tit. 21, §§ 1976(A), 1977(A) (West Supp. 1997) (Felony and Misdemeanor, depends on quantity)
38.	Oregon	Or. Rev. Stat. § 164.865 (1990 & Supp. 1998) (Misdemeanor)
39.	Pennsylvania	18 Pa. Cons. Stat. Ann. § 4116(b), (d) (West 1983 & Supp. 1998) (1st offense Misdemeanor, Felony)
40.	Rhode Island	R.I. Gen. Laws § 6-13.1-15(a)(1), (3) (1992) (Felony)
41.	South Carolina	S.C. Code Ann. § 16-11-910(A) (Law Co-op. 1985 & Supp. 1997) (Felony)
42.	South Dakota	S.D. Codified Laws § 43-43A-2 (Michie 1997) (Felony)
43.	Tennessee	Tenn. Code Ann. § 39-14-115(a)(2) (1997) (Felony)
44.	Texas	Tex. Bus. & Com. Code Ann. § 35.92(a) (West Supp. 1999) (Felony)
45.	Utah	Utah Code Ann. § 13-10-4 (1996) (Misdemeanor)
46.	Vermont	No Statute
47.	Virginia	Va. Code Ann. § 59.1-41.3 (Michie 1998) (Felony and Misdemeanor, depends on quantity)
48.	Washington	Wa. Rev. Code Ann. § 19.25.020 (West 1999) (Felony)
49.	West Virginia	W. Va. Code § 61-3-50(a), (d) (1997) (Felony and Misdemeanor, depends on quantity)
50.	Wisconsin	Wis. Stat. Ann. § 943.207 (West Supp. 2000) (Felony and Misdemeanor, depends on quantity)
51.	Wyoming	Wyo. Stat. Ann. §§ 40-13-202(a)(i), -204 to -205 (Michie 1999) (Felony)
52.	Puerto Rico	P.R. Laws Ann. tit. 33, §§ 2168-2171 (Supp. 1995-1996) (Felony)