Min Ae Yu, Ryan Lehrer, and Whitney Roland
Intellectual Property Crimes
45 Am. Crim. L. Rev. 665 (2008)

Intellectual property accounts for a large part of today's economy. n1 Protecting the rights of intellectual property owners is, therefore, a critical task of the federal government in the current environment where the distribution of illegitimate goods [*667] can be achieved on scales like never before. n2 While owners of intellectual property can protect their rights by pursuing civil remedies, the threat of civil sanctions is often insufficient to deter infringing activities. n3 Some intellectual property thieves simply view civil damages as another cost of doing business. n4 Moreover, because the theft of intellectual property does not involve tangible goods, and in most cases, does not require direct contact with the rights holder, many victims are unaware of the damages they sustain until an investigation is undertaken. n5 By 2000, U.S. companies had lost over $ 1 trillion from intellectual property theft n6 and that number is reportedly growing by $ 250 billion every year. n7 In addition to monetary damages, intellectual property theft may also compromise the safety of the general public due to the use of counterfeit materials in pharmaceuticals, auto parts and other such goods. n8

The marked increase in intellectual property theft, combined with the ineffective deterrence provided by civil remedies, has led the federal as well as state and local governments to enact criminal statutes to protect intellectual property. n9 Examples of the government's continuing commitment to prosecute intellectual property crimes include Operation Buccaneer," n10 a collaborative effort by the U.S. Customs Service and the Department of Justice ("DOJ"), the Joint Anti-Piracy Initiative, n11 [*668] which involves the FBI, and Operation Site Down, n12 a global campaign against organized piracy. n13 Enforcement efforts are also getting more sophisticated and aggressive. The DOJ launched Operation D-Elite in May 2005 to crack down on peer-to-peer (P2P) piracy networks. n14 In October 2006, the DOJ completed its first successful "criminal enforcement action against copyright infringement on a P2P network using BitTorrent technology." n15 Over the past few years, the federal government has steadily increased the number of criminal prosecutions of intellectual property crimes. n16

This Article examines several areas of intellectual property law that provide the bases for criminal prosecutions. Section II examines the theft of trade secrets; Section III discusses trademark counterfeiting; Section IV addresses copyright infringement; Section V examines the problems raised by online servers; Section VI looks at patent violations; Section VII discusses cable television and satellite descrambling; and Section VIII discusses sentencing for intellectual property crimes.

II. THEFT OF TRADE SECRETS

Although trade secret theft may be the largest obstacle faced by U.S. corporations in their global business, n17 no federal criminal statute dealt directly with the theft of commercial trade secrets until the enactment of the Economic Espionage Act in 1996 ("EEA"). n18 Part A of this Section discusses the EEA. Parts B through F discuss other federal statutes that have been used by prosecutors--with limited [*669] success--to penalize the misappropriation of trade secrets. These include the National Stolen Property Act, the Trade Secrets Act, the Mail and Wire Fraud statutes, and the Racketeer Influenced and Corrupt Organizations Act. Finally, Part G describes various state attempts to combat trade secret theft.

A. Economic Espionage Act of 1996

In response to the growing efforts by foreign governments to misappropriate the trade secrets of U.S. companies, Congress enacted the EEA in October 1996 that provided for criminal as well as civil penalties against the theft of trade secrets. n19 The statute, however, is not limited to prosecuting the theft of trade secrets by foreign governments or foreign companies. n20 The EEA established two prosecutable offenses regarding the theft of trade secrets. The first offense, "economic espionage" ("ß 1831"), arises only when the theft benefits a foreign government. n21 This offense carries higher penalties than the second offense, "theft of trade secrets" ("ß 1832"), which concerns theft benefiting any person but the true owner. n22 The second offense is more general and applicable to both foreign and domestic trade secret disputes. n23

1. Definition of Trade Secret

The EEA protects "all forms and types of financial, business, scientific, technical, economic, or engineering information . . . whether tangible or intangible, and whether[,] or [no matter] how[,] stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing." n24 The EEA imposes two requirements for such information to be considered a trade secret: (i) the owner of the property must take reasonable measures to keep the property [*670] secret; n25 and (ii) the information must derive an "independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public." n26

The EEA's broad definition of trade secrets n27 allows for far-reaching protection since no additional requirements, such as wire or mail transmission, is necessary to bring a conduct within the scope of the statute. n28 The scope, however, is not without limitation. While the EEA covers information stolen in electronic form or merely memorized, n29 it is not intended to cover the transfer of general knowledge or skills learned on a job when an employee leaves one company and moves to another in the same or similar field. n30

2. Elements of the Criminal Offenses

a. Economic Espionage

Section 1831, "economic espionage," requires that the theft of trade secrets benefits a foreign government, instrumentality, or agent in some manner. n31 This type of misappropriation of trade secrets not only covers outright theft n32 or unauthorized duplication, n33 but also includes trafficking in stolen trade secrets, n34 [*671] as well as the attempt n35 and conspiracy n36 to commit these offenses. Section 1831 also includes an intent component requiring that the misappropriation be "knowingly" committed. n37

b. Theft of Trade Secrets

Section 1832, "theft of trade secrets," applies to the misappropriation of trade secrets for the economic benefit of anyone other than the true owner. n38 Unlike ß 1831, offenses are not limited to activities that benefit a foreign government. However, three prosecutorial limitations exist that are not present in the "economic espionage" offense: n39 (i) the intended benefit realized must be economic in nature; n40 (ii) the thief must intend or know that the offense will injure the rightful owner; n41 and (iii) the stolen information must be "related to or included in a product produced for or placed in interstate or foreign commerce." n42 Like ß 1831, ß 1832 also contains an intent component requiring that the misappropriation be "knowingly" committed. As interpreted by some

federal circuits, the attempt and conspiracy provisions of ß 1832 do not require the existence of an actual trade secret. n43

3. Applicability to Conduct Abroad

Section 1837 makes the EEA applicable to the theft of trade secrets or economic espionage that occurs overseas under two circumstances: (i) if the offender is under the jurisdiction of the United States or (ii) an "act in furtherance of the offense was committed in the United States." n44 The first provision of ß 1837 extends the jurisdictional reach of the federal government to U.S. citizens, [*672] permanent residents and corporations for conduct abroad even when there is no other connection with the United States. n45 The second provision enables the federal government to pursue trade secret theft outside of the country, regardless of the status of the defendant, if some part of the activity is connected to the United States. n46

4. Prosecutions Under the EEA

Most criminal actions brought under the EEA have involved domestic theft of trade secrets. n47 While there have been several actions involving foreign defendants, n48 all actions under the EEA prior to 2001 were filed under ß 1832. n49 In May 2001, the first indictment under ß 1831 was brought, and since then, two other indictments under ß 1831 followed. n50 At least one commentator foresees more aggressive use of ß 1831 by the government as a potential countermeasure against economic terrorism. n51

During the EEA's first five years, all prosecutions under the EEA required the express approval of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General of the Criminal Division. n52 The approval requirement for ß 1832 prosecutions has since lapsed, and federal prosecutors can now prosecute ß 1832 offenses without prior approval. n53 In contrast, the Attorney General renewed the prior approval requirement for prosecutions under ß 1831. n54 Economic espionage prosecutions under ß 1831, therefore, still require DOJ oversight.

[*673] *5. Defenses*

Defenses to EEA prosecutions include: (i) independent development; (ii) reverse engineering; and (iii) lack of secrecy. Though not statutorily specified in the EEA, all of these defenses are available in civil misappropriation cases and have been applied to EEA criminal prosecutions. n55

a. Independent Development

The defense of independent development may be raised when the defendant arrives at a technique similar to the trade secret exclusive of any influence from the trade secret that the defendant is alleged to have misappropriated. n56 In the civil context, the defense of independent development is a counter to improper "use" of trade secrets; where the defendant has independently developed an idea, he cannot be said to have "used" a pre-existing idea, even if both ideas are similar. n57

b. Reverse Engineering

Reverse engineering involves the "systematic breaking down of a completed process or good into its component parts in order to identify its properties and derive expertise that enables reproduction of the trade secret." n58 If a company or proprietor of a trade secret provides information to an individual that facilitates reverse engineering of the entity's product, the individual cannot be held liable for "cracking the code." However, in order to assert the reverse engineering defense, [*674] the defendant cannot unlawfully acquire the product nor violate a license agreement to re-

frain from reverse engineering. n59 Further, an individual can be held liable for posting information acquired through reverse engineering on a website or otherwise distributing it to third parties. n60

c. Lack of Secrecy

The defense of lack of secrecy may be raised in instances where the processes purported to be secret have been widely disseminated and have become readily accessible in the public domain. n61 The defense is only applicable when, at the time of obtaining the secret, the information was widely available in the public domain. The person who misappropriates the trade secret cannot immunize himself by disclosing the information to the public domain and retroactively destroying trade secret status. n62 Once the information falls into the public domain, however, any subsequent user can invoke the lack of secrecy defense even if the information was originally obtained through improper means. n63

B. National Stolen Property Act

The National Stolen Property Act ("NSPA") n64 provides criminal sanctions n65 for any person who "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." n66 In cases involving theft of confidential documents, lower federal courts have held that the NSPA can apply to the theft of tangible property containing trade secrets, n67 [*675] even though the NSPA was not designed or intended to apply to trade secret theft. n68 However, the Supreme Court has yet to rule directly on the applicability of the NSPA to trade secrets. n69

1. Transported in Interstate or Foreign Commerce

Because the NSPA was enacted under Congress's Commerce Clause n70 authority, it applies only if the stolen trade secrets have been transported or transferred in interstate or foreign commerce. n71 The purpose of the statute was to combat theft across state and foreign boundaries, previously not actionable by individual state and foreign governments. n72 Some courts require the prosecution to prove that the stolen trade secret was physically transported. n73 More recently, courts have found transportation via electronic communication to be sufficient. n74 The mere presence of a stolen trade secret in a state or country other than its original location is generally insufficient to prove transportation, though it may be convincing when combined with other circumstantial evidence. n75 Courts have found the conscious placement of items in the stream of interstate commerce to be sufficient. n76

2. Goods, Wares, or Merchandise

Courts have reached different conclusions about the scope of this section of the statute. Goods, wares or merchandise have been broadly defined as "such personal [*676] property or chattels as are ordinarily a subject of commerce." n77 Courts have held that purely intangible items, like electronic information, cannot be considered "goods, wares or merchandise" for purposes of the NSPA. n78 However, it is well settled that the theft of a trade secret in the form of intangible information is actionable when it is connected to tangible goods. n79 The NSPA does not allow for convictions based solely on attempted theft or receipt of stolen goods. n80

3. Minimum Value of $ 5000

The intent of the NSPA is to address only theft of items having substantial market value. n81 Courts have taken a variety of approaches in determining the "value" of trade secrets. Some courts look for an actual market for the products embodying the stolen trade secrets to determine their value. n82 Absent a market, courts look for "any reasonable method" of valuation. n83 Another alternative is to use the black market price. n84 Courts have allowed this minimum value requirement to be assessed at the point of transportation in interstate or foreign commerce, [*677] rather than at the time of the theft. n85

4. Knowledge of the Same

Possession of stolen trade secrets by a defendant is not sufficient to invoke the NSPA. The government must introduce evidence establishing that the defendant knew the secret was stolen. n86 The defendant's knowledge of the illegal origin of the trade secret may be inferred from the defendant's behavior. n87

5. Stolen, Converted, or Taken by Fraud

Finally, the NSPA requires a physical theft; the "goods, wares, [or] merchandise" must actually be "stolen, converted or taken by fraud." n88

C. Trade Secrets Act

Prior to the EEA, the only federal statute that specifically addressed theft of trade secrets was the Trade Secrets Act ("TSA"), which criminalizes the unauthorized disclosure of confidential information by government employees. n89 However, because the TSA does not apply to the private sector n90 and provides only for misdemeanor sanctions, n91 federal prosecutors have traditionally relied on the NSPA and the mail and wire fraud statutes n92 to pursue charges of criminal trade secret misappropriation. n93

The TSA has been used to enjoin the government's release of technical data [*678] belonging to a government contractor. n94 However, in order for information to be considered "confidential" under the Act, the party seeking an injunction must prove that substantial competitive harm would result from disclosure of the information. n95

D. Mail and Wire Fraud Statutes

The mail and wire fraud statutes n96 provide criminal sanctions for using or attempting to use the mail n97 and wire services to perpetrate fraud. n98 Unlike the NSPA, these statutes may be applied to theft of intangibles, n99 such as trade secrets. n100

Violation of these statutes does not require the potential victims to be in fact defrauded, n101 the defendant to gain anything through the potentially fraudulent activity, n102 nor there to be reliance by the injured party. n103 Rather, violations turn on the intent to defraud the victim. n104

Under the statutes' broad definition of property, n105 appellate courts have upheld convictions involving intellectual property under the mail and wire fraud statutes [*679] even when there was no violation of the NSPA. n106 However, under these statutes, the use of the mail or wires is necessary for there to be a misappropriation. n107

Recently, the mail and wire fraud statutes have been used to give owners of intellectual property standing to bring a civil claim under the Racketeer Influenced and Corrupt Organizations Act. n108

E. Racketeer Influenced and Corrupt Organizations Act

Criminal sanctions for theft of trade secrets are also available under the Racketeer Influenced and Corrupt Organizations Act ("RICO"). n109 Although many cases brought under RICO are civil actions, n110 the predicate acts necessary to sustain a RICO claim are violations of criminal law. n111 Consequently, the elements of civil and criminal RICO actions are similar. The definition of racketeering activity applicable to the theft of trade secrets includes mail fraud, n112 wire fraud, n113 activity prohibited by the NSPA, n114 and the receipt of stolen property. n115

The RICO statute further requires that there be at least two of these predicate racketeering acts within ten years to establish a pattern of racketeering activity. n116 The Supreme Court has indicated that for such acts to be RICO predicate offenses, they must be related and amount to continued activity or otherwise pose a threat of continued activity. n117

Courts generally consider six factors to determine if a pattern has been [*680] established: (i) number of unlawful acts; (ii) length of time over which acts were committed; (iii) similarity of acts; (iv) number of victims; (v) number of perpetrators; and (vi) character of unlawful activity. n118

F Computer Fraud and Abuse Act

Section 1030 of Title 18 of the U.S. Code, n119 commonly known as the Computer Fraud and Abuse Act ("CFAA"), n120 provides criminal sanctions and a civil action for misappropriation of trade secrets stored on "protected computers." n121 The CFAA is not designed to deal specifically with trade secrets, but misappropriation of trade secrets may violate the statute. n122

Three sections of the CFAA are particularly relevant to trade secrets. Section 1030(a)(2)(c) prohibits obtaining, without authorization, information from protected computers via an interstate or foreign communication. n123 Section 1030(a)(4) criminalizes accessing a protected computer, without authorization, with the intent to defraud and obtain something of value. n124 Finally, ß 1030(a)(5) prohibits intentionally causing damage, n125 without authorization, to a protected computer. n126

G. State Law Provisions

In addition to the various federal statutes criminalizing the misappropriation of trade secrets, all states have enacted statutes to protect against the theft, use, or disclosure of another's trade secrets. n127 These state statutes vary greatly in their scope and sanctions. Some states have criminal codes that specifically address [*681] trade secrets. n128 Others have general criminal statutes that have been interpreted to cover trade secrets despite no explicit reference to them, use civil codes such as the Uniform Trade Secrets Act to confer protection, or both. n129 However, the scope of protection afforded by some state statutes, like the scope of the NSPA, is limited to the theft of tangible items. n130

III. TRADEMARK COUNTERFEITING

A trademark is "any distinct word, phrase, symbol, picture, or combinations thereof' that function to identify the source of a specific product and is one of the most valuable assets of a company n131 Counterfeiting is the deliberate and authorized use of a false mark that closely resembles a registered trademark. n132 It steals the identify of trademark owners, defrauds the consumers and costs the United States approximately $ 200 billion annually. n133 Counterfeiting is a lucrative crime, and it is replacing illicit drugs as the primary source of funds for criminal organizations. n134

This Section covers federal and state statutes that deal with the growing problem of trademark counterfeiting. Part A discusses the federal statute that criminalizes counterfeiting, the Trademark Counterfeiting Act of 1984, and its amendment, Stop Counterfeiting in Manufactured Goods Act, which was signed into law in 2006. It also reviews other federal statutes that may be used in conjunction with the TCA. Part B discusses state provisions that protect trademarks. Part C addresses anti-counterfeiting measures related to criminal organization and covers the trademark counterfeiting provisions of RICO and the money laundering statute.

A. Trademark Counterfeiting Act

1. Relation to the Lanham Act

In 1946, Congress enacted the Lanham Act, the civil trademark statute, to provide a comprehensive scheme of trademark protection. n135 Building on the [*682] Lanham Act, Congress passed the Trademark Counterfeiting Act ("TCA") of 1984 to criminalize the intentional trafficking of counterfeit goods or services. n136 In drafting the TCA, Congress relied on concepts and definitions of the Lanham Act and indicated that the TCA should be interpreted against the background of the Lanham Act. n137 Only conduct that is prohibited by the Lanham Act is criminalized by the TCA. n138

2. The 2006 Amendment

While interpreting the TCA, courts found an ambiguity in the statute. n139 Circuits split over what constituted "goods" for the purpose of the TCA. n140 The judicial split created a "loophole" as people trafficked labels and component parts, rather than the whole good, to circumvent the TCA. n141 The newly enacted amendment, Stop Counterfeiting in Manufactured Goods Act ("SCIMGA"), n142 closes the loophole by prohibiting the trafficking of counterfeit "labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentations, or packaging of any type or nature" n143 even if those phony marks are not associated with any goods. The SCIMGA also expands the definition of "trafficking" to include the import or export of counterfeit goods or distribution of counterfeit goods for private financial gains. n144 SCIMGA broadly defines "financial gains" to include "expected receipt" of "anything of value." n145 Thus, possession of counterfeit marks or goods, without actual sale or distribution, becomes a crime if the possessor intents to distribute the counterfeit material later or attempts to make a sale but failed.

3. Elements of Criminal Offense

Prior to the enactment of the SCIMGA, to prove a violation, the government had to establish that: (i) the defendant trafficked or attempted to traffic in goods or services; (ii) such trafficking or attempt was intentional; (iii) the defendant used a counterfeit mark on or in connection with such goods or services; and (iv) the defendant knew that the mark so used was counterfeit. n146 After the SCIMGA, the [*683] first element of the above requirements is expanded to include any kind of "label", and the definition of "trafficking" is expanded to cover more economic activities. n147

Congress made two exceptions to the use of a mark on allegedly counterfeit goods: (i) when the goods themselves are genuine but display a false mark; and (ii) when legitimately manufactured goods are sold beyond a licensee's license period. n148 The SCIMCA also emphasizes protection for "repackaging of genuine goods or services not intended to deceive or confuse." n149

To convict under the TCA or SCIMGA, the government does not have to prove that a defendant had criminal intent: n150 Additionally, the government may prosecute individuals for conspiracies to violate the statutes: n151

4. Defenses

Although it is disputable how valuable Lanham Act precedent is in TCA cases, the TCA does incorporate the defenses of its civil counterpart. n152 These defenses include equitable defenses such as laches, unclean hands, estoppel, fraud in obtaining the trademark registration, use of mark in violation of antitrust laws, invalid trademark, abandonment, misrepresentation, fair use, unregistered good faith prior use, and registered prior use. n153

Although the TCA and SCIMGA define a counterfeit mark as one "likely to cause confusion, to cause mistake, or to deceive," n154 courts have rejected the argument that the actual purchaser must not have been confused or deceived by the [*684] counterfeit mark as purchaser confusion is not a solitary consideration in trademark violation cases. n155

5. Other Federal Statutes

Other federal crimes that can be used to prosecute trademark counterfeiting in addition to or in lieu of the TCA include: 1) conspiracy and aiding and abetting; n156 2) mail and wire fraud; n157 3) copyright infringement; n158 4) trafficking in counterfeit labels, illicit labels, or counterfeit documentation or packaging; n159 5) trafficking in misbranded food, drugs and cosmetics; n160 6) tampering with Consumer Products; n161 and 7) trafficking in mislabeled wool, fur and textile fiber products. n162

B. RICO and Money Laundering Acts

Like theft of trade secrets, trademark counterfeiting is also illegal under RICO and the money laundering statute. n163 In 1994, Congress added trademark counterfeiting to the list of unlawful activities under the money laundering statute. n164 Similarly, the Anticounterfeiting Consumer Protection Act of 1996 made trademark and copyright counterfeiting a predicate offense under RICO n165 Congress [*685] determined that the TCA "has been proven to be an inadequate remedy for the explosive growth of criminal commercial counterfeiting" n166 and responded by amending the RICO statute to allow the government to prosecute organized criminal activity as a whole "rather than merely react to each crime the organization commits. n167

Penalties for violations of the RICO and money laundering statutes are significantly more severe than those under the TCA. n168 While the more recent amendments do not expand the definition of conduct that is illegal under the TCA, and do not necessarily increase penalties associated with criminal conduct, their provisions do increase penalties when used to prosecute organized crime. n169 Thus, under RICO, fines can be up to twice the gross profits or other proceeds of the activity. n170 Similarly, the penalty for a money laundering violation is a maximum sentence of twenty years and a maximum fine of $ 500,000, or twice the amount involved in the transaction, whichever is greater. n171 In addition to fines and imprisonment, the amended RICO statute allows law enforcement officials, including customs agents, to seize counterfeit goods and any "personal or real estate assets connected with the criminal enterprise." n172

IV. COPYRIGHT

Part A of this Section discusses the Copyright Act and emphasizes the elements of the criminal copyright infringement offense, affirmative defenses to prosecution under the Act, and the ramifica-

tions of reverse engineering. Parts B through E describe the application of the NSPA, mail and wire fraud statutes, RICO, and the money laundering statute to criminal copyright infringement. Part F discusses recent attempts to enact legislation that extends copyright protection to computer databases and other collections of information.

A. Copyright Act

The Constitution grants Congress the power to legislate in the area of copyrights. n173 Criminal copyright infringement, punishable under 17 U.S.C. ß 506, differs from civil violations because the infringing conduct must be willful and for [*686] profit. n174 The criminal copyright statute has been frequently amended as Congress endeavors to strengthen the Copyright Act and broaden its scope. n175 The Copyright Act of 1976 relaxed the mens rea prerequisite by requiring that the infringement be undertaken willfully and for purposes of "commercial advantage" or "private financial gain," rather than "for profit." n176 In 1982, Congress increased the sanctions for criminal infringement, codifying stricter fines for criminal infringement in a separate statute. n177

Enacted in October 1992, the Copyright Felony Ace n178 responded primarily to the growing problem of large-scale computer software piracy. n179 Prior to the passage of this Act, only unauthorized copying of sound recordings, motion pictures, or audiovisual works constituted a federal felony. n180 The Copyright Felony Act protects all copyrighted works and lowered the numerical and monetary thresholds for felony sanctions. n181 The mens rea requirement remained unchanged. n182

Under 17 U.S.C. ß 102, a copyright cannot exist before an expression is captured in a fixed, tangible medium. n183 As a result, musical and dramatic [*687] performances may not be protected by copyright until they are recorded. An artist's interest in his performance is protected against unauthorized recording by 18 U.S.C. ß 2319A, the anti-bootlegging statute, which applies both fines and imprisonment to penalize bootlegging, recording, reproduction, transmission, and distribution--whether for sale or not--of live musical performances. n184 The Family Entertainment and Copyright Act of 2005 n185 applies fines and imprisonment for "any person who, without the authorization of the copyright owner, knowingly uses or attempts to use an audiovisual recording device to . . . copy a motion picture or other audiovisual work protected under Title 17, . . . from a performance of such work in a motion picture exhibition facility." n186

The No Electronic Theft Act ("NET Act"), enacted in December 1997, n187 removed the "financial gain" requirement and made illegal reproduction or distribution of copyrighted materials a federal crime. n188 The prosecution must show that the infringer acted for commercial advantage or private financial gain, or that she reproduced or distributed, during any 180-day period, one or more copies of copyrighted works with a total retail value of more than $ 1000. n189 Thus, the criminal copyright statute now reaches those infringers who act solely to harm another, or for nonfinancial gratification. n190 However, criminal copyright cases that do not involve a profit motive or commercial advantage have been a rarity. n191

The Digital Millennium Copyright Act ("DMCA") n192 provides liability limitations for transmitting copyrighted material online. n193 The DMCA also provides [*688] criminal penalties n194 for circumvention of copyright protection systems n195 and for compromising the integrity of copyright management information. n196 The first indictment under the DMCA was brought in August 2001, n197 and there have been at least five additional criminal convictions under this statute. n198 The digital age has seen more international intellectual property infringe-

ments. n199 The United States recently ratified the Convention on Cybercrime, an international treaty aimed at combating computer crimes, including copyright infringements, through the Internet. n200

18 U.S.C. ß 2318 makes it a crime for individuals, without the authorization of the copyright owner, to knowingly traffic in counterfeit or illicit labels affixed to copyrighted goods, such as a phonorecord; or copies of items such as computer programs; motion pictures; audiovisual works; literary works; pictorial, graphic or sculptural works; visual art; or documentation or packaging; or counterfeit documentation or packaging. n201 It includes offenses committed within the United States, as well as those facilitated through the use of the mail or a facility of interstate or foreign commerce. n202

1. Elements of the Offense

The government bears the burden to prove four elements in a criminal prosecution for copyright infringement under 17 U.S.C. ß 506: (i) a valid copyright; (ii) infringement of that copyright; (iii) willfulness; and (iv) either (a) the infringement was for purposes of commercial advantage or private financial gain, or (b) the infringer reproduced or distributed, during any 180-day period, one or more copies or phonorecords of one or more copyrighted works, with a total retail value of more than $ 1,000. n203 The elements of a 17 U.S.C. ß 1101 violation [*689] for bootlegging sound recordings or music videos of live musical performances are similar. n204

a. Existence of a Valid Copyright

The first element of the criminal copyright offense is the existence of a valid copyright. n205 A certificate of registration issued within five years after first publication of a given work constitutes prima facie evidence of a valid copyright. n206 Presentation of the certificate shifts the burden to the defendant, who can then challenge its validity by showing that the copyright was obtained by fraud, that the registration certificate is not genuine, or that the work cannot be copyrighted. n207 However, registration of a copyrighted work is not a prerequisite for obtaining copyright protection. n208

b. Infringement

The second element, infringement, is the threshold requirement for both criminal and civil copyright infringement cases. n209 Copyright infringement can be proven by either direct n210 or indirect evidence showing that the defendant had access to the copyrighted work and that the alleged copy is "substantially similar" in idea and in expression of idea. n211 The copyright infringement element may be [*690] established even if the person distributing the infringing work did not personally produce the copies. n212

The substantial similarity test is a two step analysis that requires: (i) a showing of substantial similarity in the basic ideas involved, established by focusing on specific "extrinsic" criteria, such as the type of work involved, the materials used, the subject matter, and the setting for the subject; and (ii) a showing that the defendant's alleged copy expresses the same "intrinsic" substance and value as the original work. n213

Courts may also employ the "virtual identity" standard n214 instead of the substantial similarity test, which allows the potentially infringing work to be broken down into protected and unprotected elements which are then compared to elements of the original work. The virtual identity test looks at the two works as a whole to determine if they are virtually identical. n215 Virtual identity may be a

more useful standard for determining infringement in "reverse engineering" cases, whereby programmers dissect legally obtained software into functional elements, and use those elements to create "virtually identical" software programs which are not exact copies of one another. n216

[*691] Other courts allow allegedly infringing work to be separated from noninfringing work by filtering out copyright-protected material from non-protected components. n217 When determining whether non-literal elements n218 of computer programs are substantially similar in copyright infringement cases, courts may apply the Abstraction-Filtration-Comparison method. n219 The first step of this method involves breaking down the allegedly infringing program into its constituent structural parts and isolating each level of abstraction contained within that structure. n220 Next, the protected expression is filtered from non-protected material. n221 The final phase involves a comparison of the material structure of the allegedly infringing program with the protected core of the original work to determine if the two works are substantially similar. n222 However, when an idea can be expressed in only a minute number of possibilities, the idea itself is considered merged with the method of expressing the idea, thus barring filtration and copyright protection. n223

It is not infringement for the owner of a copy of a computer program to make, or authorize the making of, a copy or adaptation, if such a step is deemed essential to [*692] using the program, or if the step is solely for archival purposes and the copy can be destroyed if necessary. n224 It is also not infringement for the owner or lessee of a machine to make, or authorize the making of, a copy of a computer program solely by virtue of the activation of the machine that contains a lawful copy of the program, for the purposes of maintenance or repair, if such new copy is destroyed immediately after the completed maintenance or repair. n225

c. Willfulness

The third element of the criminal copyright offense is "willfulness." n226 A majority of the courts have interpreted the term to mean that the government must show the defendant specifically intended to violate copyright law; n227 however, the Second Circuit once took a different view, holding that "willfulness" requires only an intent to copy, rather than an intent to infringe. n228

[*693] *d. Financial Gain or Threshold Violation*

Congress, in passing the No Electronic Theft Act in 1997, modified the fourth element of the criminal copyright offense to require the government to show either an intent to obtain commercial advantage or financial gain, or, in the absence of an intent to obtain financial gain, the actual reproduction or distribution of one or more copies with a total value in excess of $ 1000. n229 Courts can find intent, and thus punish the defendant, when he commits the violation for the purpose of financial gain, whether or not that gain is realized. n230 Acts performed to achieve gain may involve monetary transactions or bartering for other protected materials. n231

2. Defenses

While the criminal copyright infringement statute does not provide explicit statutory defenses, civil defenses are available. n232 One potential defense is the "first sale" doctrine. n233 According to this doctrine, upon sale, the author conveys title of the particular copy of a copyrighted work and abolishes his right to restrict subsequent sales of that particular copy. n234 The purchaser does not, however, gain [*694] the right to reproduce and distribute additional copies of the work. n235

Further, the benefits of the doctrine do not extend to rental or loan arrangements. n236 Included in the protection of the first sale defense are copies that were imported into the United States. n237

Another defense, fair use, applies an "equitable rule of reason" n238 analysis requiring the balancing of factors to protect the copyright owner, while still promoting the purpose behind copyright laws, namely fostering creativity. n239 No bright line test exists for determining whether any particular use is a "fair use" rather than an act of infringement, so each use requires a case-by-case determination. n240 Factors considered by a court to determine if a fair use defense exists include: (i) the purpose and character of the use, including whether it is of a commercial nature or for non-profit educational use; (ii) the nature of the copyrighted work; (iii) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (iv) the effect of the use upon the potential market for, or value of, the copyrighted work. n241 A defense of fair use as parody n242 [*695] requires an examination of the expressive intent of the infringing work to determine if it has a "critical bearing on the substance or style" of the original work. n243 Reverse engineering can also be fair use when it is the sole route to access ideas and functional elements of a copyrighted computer program. n244 The Family Movie Act of 2005 n245 allows editing of DVD movies to create "sanitized" versions, but does not allow creation of new hard copies or insertion of replacement footage.

3. Penalties

The basic offense of copyright infringement involving sound recordings, phonorecords, motion pictures, and audiovisual works now carries a sentence of up to five years in prison. n246 Any subsequent offense increases the penalty to up to ten years of imprisonment. n247

The Copyright Damages Improvement Act of 1999 compelled changes in the U.S. Sentencing Guidelines ("Guidelines"), which further impacts statutory penalties. n248 The Guidelines increased the base offense level to eight. n249 Enhancement is permitted for offenses involving "manufacture, importation, or uploading of infringing" works. n250 The offense level is further increased if the infringement amount exceeds $ 2000. n251

Violations of 18 U.S.C. ß 2318 carry criminal penalties of fines, imprisonment of not more than five years, or both. n252 When a person is convicted of violating 18 [*696] U.S.C. ß 2318(a), the court is also required to order the forfeiture, destruction, or disposition of all counterfeit or illicit labels and all articles to which such labels are affixed, as well as any equipment or material used to facilitate these activities. n253 A copyright owner who is injured, or threatened with injury, can bring a civil action in an appropriate U.S. District Court. n254 The court, at its discretion, may grant an injunction; order the impounding of any articles used to violate this statute; award the injured party reasonable attorney fees and cost; and award either actual damages plus profits realized by the copyright infringer or statutory damages in an amount between $ 2,500 and $ 25,000. n255 This award may be increased by three times the amount awarded if the court finds that an individual has violated subsection 18 U.S.C. ß 2318(a) within three years after final judgment for a violation of that subsection. n256

The Family Entertainment and Copyright Act of 2005 provides for fines, imprisonment of not more than three years, or both. n257 The penalty for a subsequent offense is a fine and imprisonment of not more than six years. n258 As with 18 U.S.C. ß 2318, this statute also orders the forfeiture or destruction of all unauthorized recordings and devices and equipment used in connection with the offense. n259 In addition, an owner or lessee of a motion picture theater may detain, for a

reasonable time period, any person suspected of violating this statute without liability for the detention. n260

4. Reverse Engineering

Reverse engineering is the process where a protected work is broken down to its component and non-protected parts, from which a similar, competitive product may be created. n261 Because only the expression of an idea, and not the idea itself, may be protected under copyright law, n262 reverse engineering may not constitute copyright infringement. Reverse engineering is a fair use when it is the sole route to access ideas and functional elements of a copyrighted computer program, and when there is a legitimate reason for doing so, n263 i.e., "for the sole purpose of [*697] identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs." n264 The anti-circumvention provisions of the DMCA also contain an exception for reverse engineering. n265

B. National Stolen Property Act

In the past, courts extended the protections of the National Stolen Property Act ("NSPA") n266 to copyrighted goods. n267 This extension was effectively overruled by *Dowling v. United States*, n268 where the Supreme Court held that the NSPA does not prohibit the interstate transportation of goods infringing on another's copyright. n269 Because there had been no actual physical removal or theft of the property, the Court held that the NSPA's requirement that the goods be "stolen, converted or taken by fraud" was not met. n270

C. Mail and Wire Fraud Statutes

The mail and wire fraud statutes n271 impose criminal penalties on those who utilize the mail or wires to defraud others through copyright infringement. n272 To establish a violation of either statute, the government must meet the same criteria as set out in Section II.D. Additionally, one district court has held that federal [*698] copyright law does "not necessarily preempt other proprietary rights." n273 Because the defendants in that prosecution would not profit from their infringement until transmission by wire had occurred, the court held that remedies were not limited to those provided by the copyright statute, and that prosecution under the wire fraud statute was acceptable. n274

D. Racketeer Influenced and Corrupt Organizations Act

The Anti-Counterfeiting Consumer Protection Act of 1996 amended RICO, and made copyright counterfeiting a racketeering activity. n275 Copyright infringement claims can be brought under RICO n276 if the infringing acts continue over a period of time, and relate to each other in a common plan created by the violators with the intent to defraud. n277

E. Money Laundering Act

The money laundering statute, 18 U.S.C. ß 1956, defines money laundering, and includes the receipt of proceeds from trafficking in counterfeit goods, or goods infringing on a copyright, as specified unlawful activities. n278

F. Database Protection

Copyright law currently provides minimal protection for databases. n279 The *Feist* decision established that merely expending the effort to assemble data is insufficient to qualify the compilation for copyright registration, n280 but this decision "did not have a major impact" on the U.S. Copy-

right Office's registration practices for [*699] compilations. n281 The U.S. Copyright Office allows databases to be registered as copyrighted providing that the databases constitutes "original authorship"; when there is some doubt of this, the Office issues a registration under its "rule of doubt," which formally doubts the copyright ability of the database. n282

Several international treaties protect databases, assuming the databases are copyrightable. n283 The Berne Convention for the Protection of Literary and Artistic Works, which the United States has joined, requires member countries "to protect collections of literary or artistic works such as encyclopedias and anthologies which, by reason of the selection and arrangement of their contents, constitute intellectual creations.'" n284 Furthermore, databases of fact are covered by the 1995 Trade-Related Aspects of Intellectual Property Rights ("TRIP") Agreement, which states: "[c]ompilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such." n285 The World Trade Organization has been bound by this obligation since January 1996. n286

G. State Law Provisions

State criminal copyright laws are largely pre-empted by federal law if the conduct would also be considered criminal infringement under the Copyright Felony Act. n287 17 U.S.C ß 301(a) subjects all state criminal copyright laws to preemption where they create legal and equitable rights equivalent to any of the exclusive rights under 17 U.S.C ß 106, and with respect to copyrightable works created prior to 1978. Only if the right conferred by state law is not included within the scope of the Copyright Act does state law prevail. n288 The exception for works created prior to 1972 n289 is co-terminus with the term of statutory renewal of copyright protection, and will expire ninety five years from first publication under the Copyright Term Extension Act of 1998 ("CTEA") and 17 U.S.C ß 304(b). n290

[*700] V. ONLINE SERVERS: CRIMINAL VIOLATIONS OF THE COPYRIGHT FELONY ACT

This Section outlines the application of the Copyright Act to online activities. Part A discusses criminal liability of individuals who transfer files in cyberspace, emphasizing conduct that constitutes infringement, the financial gain (or thresh-old) requirement, and the first sale doctrine. Part B discusses Internet Service Providers' liability for activities on their networks.

A. Individual Criminal Liability

A criminal violation of the Copyright Act occurs when one willfully reproduces or publicly distributes any kind of copyrighted work. n291 The Copyright Act of 1976 n292 protects the use of text files, n293 image files, n294 and sound files n295 on the Internet. n296 Criminal copyright infringement that: (i) is facilitated by or achieved through the Internet; and (ii) meets the statutorily prescribed number of copies or dollar value, may lead to felony prosecution. n297 Making a work for commercial distribution available for distribution on a computer network for public access also constitutes infringement if the perpetrator knew or should have known that the work was intended for commercial distribution. n298 Penalties for distributing a commercial work through a public computer network include heightened maximum sentences for repeat offenses and offenses committed for commercial [*701] advantage or personal financial gain. n299 These added protections were in response to the growing demand for additional protection of digital works in cyberspace. n300 This Section addresses: (i) conduct over the interne that constitutes infringement; (ii) the prob-

lematic application of the "first sale doctrine" exception; and (iii) the statutory requirements of intent and commercial or financial gain in establishing criminal liability.

1. Infringement via the Internet

Unauthorized file transfers of copyrighted materials infringe on the copyright holder's exclusive rights in two ways: uploading n301 files, which violates the rights of distribution, n302 and downloading n303 files, which violates reproduction rights. n304

In *A&M Records, Inc. v. Napster Inc.*, the Ninth Circuit held that such conduct [*702] does not constitute fair use. n305 First, sending a file to an anonymous requester cannot be considered a personal use, since the purpose of saving the expense of purchasing copies is more properly viewed as commercial. n306 Second, copying an entire work weighs against a finding of fair use. n307 Courts have refused to acknowledge unauthorized sampling as fair uses, and have split as to whether space-shifting is a fair use in the context of file transfers. n308

The Seventh Circuit dealt with these issues in *In re Aimster Copyright Litigation*. n309 The Aimster service was similar to Napster in many respects, but notable in that the Aimster service did not use its own servers to copy or house copyrighted music files. n310 In the opinion by Judge Richard Posner, the Seventh Circuit noted that ultimate liability in cases of alleged contributory infringement would depend on whether or not there are non-infringing uses for which Aimster may be used, and "how probable" those uses are. n311 The court was "unwilling to allow copyright holders to prevent infringement effectuated by means of a new technology at the price of possibly denying non-infringing consumers the benefit of the technology." n312

In addition, copyright infringement can also be found where a computer makes copies to a random access memory (RAM) device. n313 In *Tiffany Design, Inc. v. Reno-Tahoe Specialty, Inc.*, the District Court of Nevada held that when the defendant's designer scanned in all or at least a large portion of the copyrighted picture into the defendant's computer's RAM, an unauthorized copy was made, constituting an act of copyright infringement. n314 Even though the picture was scanned for derivative work, the court still found a violation of the Copyright [*703] Act. n315 The court enunciated its holding very clearly by stating: "the digitization or input of any copyrighted material, whether it be computer code or visual imagery, may support a finding of infringement notwithstanding only the briefest existence in a computer's RAM." n316

2. The Financial Gain Requirement or Threshold Violation

The NET Act of 1997 amended 17 U.S.C. ß 506(a) to permit the government to prove either financial gain, or reproduction or distribution, including by electronic means, during any 180-day period, of one or more copies of one or more copyrighted works whose total retail value exceeds $ 1,000. n317 Moreover, the definition of "financially motivated transactions" includes trading infringement material for other copyrighted works. n318 However, the 2005 amendment to 17 USC ß 506(a) does not require proof of financial gain by distributing a work prepared for commercial distribution through a public computer network. n319 Additionally, the defense of fair use under section 107 is rebutted by showing that the use was commercial or for financial gain. n320

3. The Internet and the First Sale Doctrine

The first sale doctrine allows an owner of a copy of a copyrighted work to legally sell or give away his copy of that work. n321 Applying this doctrine to file transfers in cyberspace, a person

who legally installs or downloads a copy of a file to his own disk may freely redistribute that copy, whether or not he assesses a fee, to anyone else by sending the file and then deleting his copy. n322

[*704] A split in views exists where a copy is lawfully downloaded to a computer, rather than to a disk. Some argue that it is permissible to subsequently transmit the file provided that the initial purchaser deletes the copy on his computer at substantially the same time as he transmits a copy to another. n323 Others maintain that this still violates the exclusive rights of the copyright owner. n324 Courts are also divided on whether the first sale doctrine is an affirmative defense, which the defendant has the burden of proving, or whether the absence of a first sale is an affirmative element of the government's prosecution. n325

B. Internet Service Provider Liability

Criminal liability for copyright infringement is predicated on a finding that the alleged perpetrator acted willfully. n326 The cyberspace context complicates this finding because an Internet service provider (ISP) can convincingly argue an unknowing contribution to, or commission of, an offense. n327 The expansion of copyright law to address the Internet has yielded civil cases involving allegations of copyright infringement against ISPs for contributory n328 or vicarious n329 copyright [*705] infringement. The Supreme Court's recent decision in *MGM Studios v. Grokster* n330 speaks directly to this point and has widespread implications for third party liability. In *Grokster*, the Court held that an entity can be found liable for contributory infringement if it knowingly and intentionally distributes a product with the principal purpose of promoting infringement. n331 Liability can attach even if the product has substantial non-infringing uses. n332 Although seemingly contradictory to the Court's, earlier ruling in *Sony Corp. of America v. Universal City Studios*, n333 which precluded third party liability for the distribution of a commercial product capable of infringement, the Court in *Grokster* distinguished *Sony*, finding that when evidence goes beyond a product's potential or capability for infringement and shows actions directed at promoting infringement, the *Sony* rule will not preclude liability. n334

Congress, however, has provided a "safe harbor" to ISPs through the Digital Millennium Copyright Act ("DMCA"). n335 In general, the DMCA exempts an ISP n336 from liability for monetary, injunctive, or other equitable relief for copyright infringement because of the provider's transmitting, routing, or providing a connection for such material, or temporarily storing such material [*706] in the course of such a transmission, routing, or connection. n337 The provider remains exempt from liability for copyright infringement so long as the provider has no "actual knowledge" of the infringement, is not aware of information indicating that the material is infringing, and "does not receive a financial benefit directly attributable to the infringing activity." n338 Although the law does not require a provider to monitor or otherwise seek out information indicating infringement, the law does require that a provider, upon obtaining such information, expediently remove or disable access to such material. n339 Those who knowingly and materially misrepresent that the material is infringing, or that the material was removed, disabled by mistake, or misrepresented, are liable for damages. n340 Where a provider removes or disables access to such material in "good faith," or based on circumstances "from which infringing activity is apparent, regardless of whether the material is ultimately determined to be infringing," the provider will generally n341 not be liable. n342 It is unlikely, however, that peer to peer service providers [*707] who meet the DMCA requirements of an ISP would receive statutory safe harbor. n343

VI. PATENT

A patent is a government issued document granting the holder of the patent the exclusive right to use an invention or design. n344 This Section is divided into three parts. Part A discusses criminal liability for false patent marking. Part B discusses counterfeiting and forging of letters patent. Finally, Part C discusses whether the National Stolen Property Act applies to patent infringement.

While most federal remedies for patent misuse are civil, the Patent Act also establishes criminal liability for infringement. n345 Although the Patent Act authorizes both government and private action, the government rarely initiates claims for Patent Act violations, leaving it to private parties to bring the majority of patent infringement suits.

A. False Marking

False marking includes false affixing, marking, or use in connection with sales or advertising of: (i) the name or any imitation of the name of the patentee; (ii) the patent number; or (iii) the words "patent" or "patentee." n346 Additionally, the use of the word "patent," or any word or number indicating that the item is patented, in connection with a non-patented item violates this statute, as does the use of the words "patent applied for," "patent pending," or any other words falsely conveying the status of a patent. n347

An element of criminal liability under 18 U.S.C. ß 292 is the defendant's specific intent to deceive the public. n348 The government may prove specific intent to deceive the public by showing that the defendant did not reasonably believe that [*708] the items were properly marked as covered by the indicated patent. n349 This objective standard may be shown by proving misrepresentation and the defendant's knowledge of the misrepresentation. n350

B. Counterfeiting or Forging Letters Patent

The Letters Patent statute imposes criminal sanctions for persons forging, counterfeiting, or altering any patent, as well as persons knowingly passing, uttering, or publishing as genuine any such patent. n351 Punishments for violation of the statute are fines and imprisonment up to ten years. n352

C. National Stolen Property Act

Dowling v. United States n353 excluded interstate transportation of goods infringing on another's copyright from the coverage of the National Stolen Property Act ("NSPA"), n354 and implied, and has been interpreted to mean, that the Act also does not apply to the interstate transportation of goods infringing on patents. n355 Because patent infringement, like copyright infringement, does not constitute a physical taking, the Supreme Court took a literal view of the Act's requirement that the goods in dispute be "stolen, converted or taken by fraud." n356

VII. CABLE TELEVISION AND SATELLITE DESCRAMBLING

This section discusses the application of federal criminal wire tap laws to cable television and satellite descrambling. n357 18 U.S.C. ß 2512(1)(a) makes it illegal for [*709] any person to intentionally possess, send through the mail, assemble, or sell a device that circumvents, unscrambles, or intercepts wire, oral, and electronic communications placed in interstate commerce. n358 Cable television and satellite descrambling are prohibited under federal wire tap laws and the Electronic Communications and Privacy Act of 1986 ("ECPA"). n359 The ECPA requires intent n360 and knowledge that the device's primary use is for surreptitious interception. n361 The law makes it illegal to advertise the sale of such devices in newspapers, magazines, other publications, or through electronic means such as the Internet. n362 In contrast to other intellectual property criminal stat-

utes, the descrambling law does not distinguish between commercial and non-commercial offenders. n363

VIII. SENTENCING

This Section covers the provisions of the U.S. Sentencing Guidelines ("Guidelines") applicable to the following statutes: n364 the EEA, the NSPA, the Trade Secrets Act, the Mail and Wire Fraud statutes, RICO, the TCA and Copyright Felony Act, False Marking and Counterfeiting or Forging Letters Patent statutes, and Cable Television and Satellite Descrambling statute. Because a defendant may be criminally liable under any combination of these statutes, the grouping analysis must be considered when determining the defendant's sentence after a multi-count conviction. n365

[*710] *A. Economic Espionage Act of 1996*

Defendants convicted of violating 18 U.S.C. ß 1831 may be imprisoned for a maximum of fifteen years, fined $ 500,000, or both. n366 Those convicted of violating ß 1832 may be imprisoned for up to ten years, fined $ 500,000, or both. n367 Defendants are sentenced under U.S.S.G. MANUAL ß 2B1.1, n368 which permits an increase by two offense levels for trade secret theft where the defendant knew or intended that it would benefit a foreign government, instrumentality, or agent. n369 Although the Economic Espionage Act (EEA) mandates forfeiture of any proceeds or property derived from violations, property used to commit or facilitate the commission of the crime is forfeited only at the discretion of the court. n370 State law provides additional relief and the EEA specifically states that it does not "preempt or displace any other remedies, whether civil or criminal." n371

B. National Stolen Property Act

The NSPA imposes a maximum imprisonment term of ten years, a fine determined under Title 18 of the U.S. Code, or both. n372 Defendants are sentenced under section 2B 1.1, n373 which provides that the base offense level of six applies where the total loss to the victim is $ 5,000 or less. n374 The offense level rises as the financial loss to the victim increases, with a maximum increase of twenty-six levels for losses exceeding $ 100 million. n375 Additionally, if the defendant is in the business of receiving and selling stolen property, the level is increased by two. n376

[*711] *C. Trade Secrets Act*

Violations of the Trade Secrets Act may result in a maximum one-year imprisonment, a fine determined under Title 18, or both. n377 In addition, the convicted person is removed from public office or employment. n378 Defendants are sentenced under section 2H3.1 of the Guidelines. n379 The base level is generally nine, but is six if the offense has a statutory maximum term of imprisonment of one year or less. n380 The base offense level of nine is increased by three if the purpose of the conduct was to obtain commercial advantage or economic gain or the defendant is convicted under 18 U.S.C. ß 1039(d) or (e). n381 The 2007 Amendments to the Guidelines make it clear that if the purpose of the conduct was to facilitate another offense, section 2H3.1 requires the application of the guideline applicable to the other offense, if the resulting offense level is greater. n382

D. Mail and Wire Fraud Statutes

Defendants convicted of mail and wire fraud risk a maximum twenty-year sentence, a fine determined under Title 18, or both. n383 If the crimes affect a financial institution, fines can increase to $ 1 million and the prison term can be lengthened to thirty years. n384 Defendants are sentenced under section 2B 1.1 or 2C1.7 of the Guidelines. n385 The base offense level of six applies where

the total loss to the victim is $ 5,000 or less. n386 As the financial loss to the victim increases, the offense level rises up to a maximum increase of twenty-six levels for losses exceeding $ 100 million. n387 Additionally, the level can be elevated by two if the offense was committed through mass-marketing n388 and by four if the crime involved a scheme to defraud more than fifty victims. n389

[*712] *E. Racketeer Influenced and Corrupt Organizations Act*

Convictions under RICO carry a maximum sentence of twenty years, a fine determined under Title 18, or both. n390 Additionally, RICO requires that the defendant forfeit any interests in enterprises established, operated, or maintained in violation of the statute. n391 Defendants are sentenced under section 2E1.1. n392 Although the Anti-Counterfeiting Consumer Protection Act of 1996 n393 broadened the scope of RICO to include intellectual property violations, it did not change the penalties.

F. Trademark Counterfeiting Act and Copyright Felony Act

Individuals convicted of violating the TCA face a prison term of not more than ten years, a fine of up to $ 2 million, or both. n394 Organizations risk a maximum fine of $ 5 million. n395 A first-time conviction for trafficking goods that bear forged or counterfeited labels may result in not more than five years imprisonment, a fine determined under Title 18, or both. n396 Upon a determination that any articles in the possession of a defendant bear counterfeit marks, the goods may be ordered destroyed and a defendant may be forced to forfeit any proceeds obtained from the offense and any property used to commit or facilitate the offense. n397

First-time offenders may be imprisoned for not more than five years, n398 fined not more than $ 250,000 for an individual, or $ 500,000 for an organization, or both. n399 Repeat offenders risk an increase in the maximum prison sentence to ten years. n400 [*713] In addition, if the offender derives personal financial gain from the offense or causes third-party financial losses, the offender may be fined no more than gross gain or twice the gross loss, whichever is greater. n401

The Copyright Felony Act was amended in 2005 to include violations for the distribution of commercial works via public computer network n402 First-time offenders for non-commercial purposes may be sentenced to a maximum of three years, n403 while first time offenders deriving commercial advantage or private financial gain may be imprisoned for a maximum of five years. n404 First time offenders for both commercial and non-commercial purposes may be fined under Title 18. n405 Repeat non-commercial offenders may be sentenced for no more than six years, while repeat commercial offenders deriving private financial gain may be imprisoned for up to ten years and fined under Title 18. n406

The Copyright Felony Act prescribes a misdemeanor sentence of a maximum one-year imprisonment and a fine not to exceed $ 100,000 for any criminal copyright infringement failing to meet the numerical thresholds described above. n407 Finally, 17 U.S.C. ß 506(b) grants the court the discretion to order the forfeiture and destruction of infringing items and all implements, devices, or equipment used in their manufacture. n408

Defendants convicted of either trademark counterfeiting or criminal copyright infringement are sentenced under section 2B5.3 of the Guidelines, n409 starting with a base offense level of eight. n410 If the infringement amount exceeds $ 5,000, the offense level rises as the financial loss to the victim increases, to a maximum increase of twenty-six offense levels for losses exceeding $ 100

million. n411 The [*714] "infringement amount" may refer to the retail value of the infringing items and not to that of the genuine items or materials; however, the retail value of the genuine items may be relevant in determining the retail value of the infringing items. n412 Pursuant to section 105 of the Family and Entertainment Act of 2005, the federal sentencing guidelines were amended to include a two level increase if the offense included the display, performance, publication, reproduction, or distribution of a work being prepared for commercial distribution. n413

G. False Marking and Counterfeiting or Forging Letters Patent

False marking violations under 35 U.S.C. ß 292 result in a maximum fine of $ 500 per offense, n414 where each false marking violation is subject to a separate fine. n415 Violations of the Letters Patent statute n416 carry a maximum ten-year term of imprisonment n417 and fines pursuant to ß 3571 of Title 18, or both. n418 Defendants convicted of counterfeiting or forging letters patent are sentenced under section 2B 1.1 of the Guidelines. n419

[*715] *H. Cable Television and Satellite Descrambling*

Cable television and satellite descrambling is punishable under the Electronic Communications Privacy Act and wire tap statutes. n420 Offenders are subject to fines under Title 18 and a maximum sentence of five years. There is no distinction between commercial and non-commercial offenders. n421 Defendants convicted under 18 U.S.C. ß 2512 are sentenced according to section 2H3.2 of the Guidelines. n422 The official commentary to the sentencing guidelines also indicates that a defendant who de-encrypts or disables technological security measures to gain access to "an infringed item" may be subject to a sentence adjustment under section 3B1.3. n423