I. INTRODUCTION ....................................................... 900

II. THEFT OF TRADE SECRETS ........................................ 901
   A. Economic Espionage Act of 1996 ............................. 901
      1. Definition of Trade Secret ............................... 902
      2. Intent and Method of Misappropriation ............... 902
      3. Tangibility ............................................. 904
      4. Prosecutions Under the EEA ............................ 904
   
   B. National Stolen Property Act ............................... 905
      1. Transported in Interstate Commerce ................... 905
      2. Goods, Wares or Merchandise ........................... 905
      3. Minimum Value of $5,000 ............................... 906
      4. Stolen, Converted, or Taken by Fraud ............... 907
      5. Knowledge that Items Were Stolen .................... 907
      6. Shortcomings of the NSPA ............................. 907
   
   C. Trade Secrets Act .......................................... 908
   
   D. Mail and Wire Fraud Statutes .............................. 908
   
   E. Racketeer Influenced and Corrupt Organizations Act .... 909
F. State Law Provisions ........................................ 910

III. TRADEMARK COUNTERFEITING ................................. 911

A. Trademark Counterfeiting Act ............................... 911
   1. Defenses ........................................... 912
   2. Operation Counter Copy ............................. 912

B. RICO and Money Laundering Acts ......................... 912
   1. Penalties .......................................... 913

IV. COPYRIGHT .......................................................... 914

A. Copyright Felony Act ........................................ 914
   1. Elements of the Offense .............................. 916
   2. Defenses ........................................... 918
   3. Reverse Engineering ................................... 920

B. National Stolen Property Act ............................... 920

C. Mail and Wire Fraud Statutes ................................. 920

D. Racketeer Influenced and Corrupt Organizations Act .... 921

E. Money Laundering Act ......................................... 921

F. The Database Protection Bill ................................. 921

V. ONLINE SERVERS: CRIMINAL VIOLATIONS OF THE COPYRIGHT FELONY ACT .... 922

A. The Internet and the First Sale Doctrine ............... 923

B. Criminal Liability ........................................... 924
   1. The "Intent" Requirement .............................. 924
   2. The Commercial Advantage/Financial Gain Requirement 925

C. Warez Sites and Internet Service Provider Liability .... 926

VI. PATENT ................................................................. 927

A. False Marking ................................................. 927

B. Counterfeiting or Forging Letters Patent ............... 928

C. National Stolen Property Act ............................... 928

VII. ART CRIMES .......................................................... 929
I. INTRODUCTION

Owners of intellectual property have great incentives to protect their rights in such property by pursuing civil remedies. Yet the possibility of civil sanctions alone is insufficient to deter violators who would steal a trade secret or infringe on another's trademark, copyright, or patent. [FN1] Indeed, some entrepreneurs view civil damage actions as just another cost of doing business. It has been estimated that the theft of intellectual property rights in the United States cost over $300 billion dollars in 1997 alone, with high technology corporations most frequently targeted. [FN2]

*901 This void in the enforcement mechanisms of intellectual property rights is filled by various federal and state criminal statutes. These are often general statutes which are interpreted to offer protection to the intellectual property at issue. Other statutes are specifically tailored to the type of intellectual property for which protection is sought. These latter provisions are used with increasing frequency to facilitate deterrence and punish perpetrators.

This article examines several areas of intellectual property law under which criminal prosecutions are brought. Section II covers the theft of trade secrets, while Section III discusses trademark counterfeiting. Next, Section IV addresses copyright infringement. Section V examines the new problems raised by online servers, while Section VI looks at patents and Section VII at art crimes. Finally, Section VIII discusses sentencing for intellectual property crimes.

II. THEFT OF TRADE SECRETS

Prior to the enactment of the Economic Espionage Act, which will be addressed in Part A, there was no federal criminal statute that dealt directly with the theft of trade secrets in the form of intangible intellectual property. The remaining Parts of this Section will cover the other statutes that federal prosecutors have used in the past, with
limited success, to penalize the misappropriation of trade secrets. Part B covers the National Stolen Property Act, while Part C discusses the Trade Secrets Act and Part D analyzes the Mail and Wire Fraud statutes. Part E addresses the Racketeer Influenced and Corrupt Organization Act, and finally, Part F describes state provisions.

A. Economic Espionage Act of 1996

In October 1996, discouraged with the failure of civil remedies in preventing trade secret theft and with the inability of prosecutors to use effectively other criminal statutes, Congress made the theft of trade secrets a federal crime with the enactment of the Economic Espionage Act ("EEA"). [FN3] The EEA established two criminal statutes with which to prosecute theft of trade secrets. The first applies only when the theft is carried out to benefit a foreign government. [FN4] This carries higher penalties than the second section, which is broader and is generally applicable to all trade secret theft. [FN5]

1. Definition of Trade Secret

The EEA defines trade secrets to include "all forms and types of financial, business, scientific, technical, economic, or engineering information ... whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing ...." [FN6] This definition is substantially similar to the one in the civil trade secret law, the Uniform Trade Secrets Act ("UTSA"). [FN7] In order to protect property that is considered a trade secret, however, the owner of the property must take reasonable measures to keep it secret. [FN8]

Additionally, the economic value of the information must be derived from the general public's lack of knowledge about it or the public's inability to readily ascertain it through proper means. [FN9] This provision imposes a higher standard of self-protection on the owner of a trade secret than on owners of any other type of property. [FN10]

2. Intent and Method of Misappropriation

The second component of the EEA, which is applicable to trade secret theft that does not benefit a foreign government, contains specific intent and methods of misappropriation requirements. Section 1832 states broadly that any unauthorized possession of a trade secret with intent to injure another violates the act. [FN11]

*FN3* The EEA intent requirements include: "knowingly" intending "to convert a trade secret," while "knowing that the offense will, injure any owner of that trade secret." [FN12] Consequently, the scope of the EEA is somewhat more limited than its civil counterpart, the UTSA, which does not require that the "defendant be aware of the trade secret." [FN13]

On the other hand, the EEA's definition of "theft" of a trade secret is broader than the UTSA's which provides simply that misappropriation is "by improper means." [FN14] The EEA definition is more expansive because it includes the mere receipt of a trade secret as a violation. [FN15]

Another expansive provision of the EEA is § 1837, which allows the government to prosecute conduct which occurs overseas if the party involved in the activity is bound by United State federal law or if an "act in furtherance of the offense was committed in the United States." [FN16] The first provision in § 1837 extends the reach of the federal government to penalize the actions of United States citizens and corporations abroad, presumably even when there is no other nexus with the United States. [FN17] The second provision enables the federal government to pursue trade secret theft outside of the country as long as some part of the activity, such as a phone call, was connected to the United States. [FN18]

At the same time, § 1833 narrows the scope of the act by providing two exceptions relating to law enforcement and other governmental activities. [FN19] The first exception allows the government to continue an otherwise lawful "investigative, *FN4* protective, or intelligence activity." [FN20] The second exception permits the reporting of suspected criminal activity to law enforcement. [FN21]
3. Tangibility

Another important provision of the EEA is its broad definition of property: "tangible or intangible, and whether or how stored." [FN22] This implies that information that is taken in electronic form or merely memorized falls under the definition of trade secret theft. [FN23] As discussed in later sections, this is the first time that federal legislation has specifically protected intangible property without additional requirements, such as a use of the mail or a wire transmission.

The EEA's legislative history indicates that the provision covering memorized information was not intended to include the general knowledge and skill learned on a job when an employee leaves a company and moves to another in the same or similar field. [FN24]

4. Prosecutions Under the EEA

Because the EEA is still a new law, the government has only begun to prosecute violators. Some commentators have speculated that the government will wait for cases where "the blatancy of the theft and the potential ease of conviction" are obvious. [FN25]

There have been reports of at least four cases where the government used the EEA to bring charges against alleged violators. In June 1997, the FBI in Philadelphia charged two Taiwanese nationals with attempting to steal trade secrets involving Taxol, a cancer-fighting drug produced by Bristol-Myers Squibb Co. [FN26] According to the FBI, these are believed to be the first two arrests brought under the EEA involving an international corporation. [FN27]

Two other reported cases filed under the EEA involve the theft of PPG Industries' glass-making process [FN28] and of a breast cancer treatment called Taximofen. [FN29] Lastly, in September 1997, the FBI in Cleveland arrested a Taiwanese businessman and his daughter in connection with the theft of trade secrets from the *905 Avery Dennison Corp. relating to formulations for self-adhesive products, initially valued at $50-60 million. [FN30]

B. National Stolen Property Act

The National Stolen Property Act ("NSPA") [FN31] provides criminal sanctions 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 ...." [FN32] The federal courts have held that the NSPA is applicable to the theft of tangible property containing trade secrets under certain circumstances. [FN33]

1. Transported in Interstate Commerce

To fall within the scope of the NSPA, allegedly stolen trade secrets must be transported or transferred in interstate or foreign commerce. [FN34] The prosecution must also prove that the stolen item was physically transported; it is not enough for the prosecution to establish the presence of a stolen trade secret in a state or country other than its original location. [FN35]

2. Goods, Wares or Merchandise

In United States v. Seagraves, [FN36] the Third Circuit defined "goods, wares or *906 merchandise" broadly as "such personal property or chattels as are ordinarily a subject of commerce." [FN37] Accordingly, the Seagraves court held that stolen maps were the subjects of commerce, albeit of a specialized nature, and were therefore "goods, wares or merchandise" within the terms of the NSPA. [FN38] Courts have also held that trade secrets must be stolen
while in a tangible form or in conjunction with tangible goods; [FN39] so a violation cannot be established if, for example, a thief merely memorizes a secret formula and then writes it down after crossing a state boundary. [FN40]

3. Minimum Value of $5,000

The intent of the NSPA is to address only the theft of items having substantial market value. [FN41] Courts have taken a variety of approaches in determining the "value" of trade secrets. Some courts have looked for an actual market for the products embodying the stolen trade secrets to determine their value. [FN42] Absent a market, courts have looked for "any reasonable method" of valuation. [FN43] The amount of time and money defendants invested in the misappropriation scheme is *907 one alternative to market value. [FN44] Another alternative is using the black market price. [FN45]

4. Stolen, Converted, or Taken by Fraud

Finally, the NSPA requires a physical theft: the "goods, wares, [or] merchandise" must be physically "stolen, converted or taken by fraud." [FN46]

5. Knowledge that Items Were Stolen

Possession of stolen trade secrets by a defendant is not sufficient to place a potential transgressor of § 2314 within the boundaries of the NSPA. The government must introduce evidence establishing that the defendant knew the items were stolen. [FN47] The defendant's knowledge of the illegal origin of the trade secret may be inferred from the defendant's behavior. [FN48]

6. Shortcomings of the NSPA

With the rapid growth of computerized digital technologies, prosecutors often had difficulties obtaining convictions under the NSPA. The intangible nature of many trade secrets has prevented the government from using the NSPA to prosecute trade secret theft since the statute is limited to "goods, wares, merchandise, securities or money" which are tangible property. [FN49]

In United States v. Brown, [FN50] the Tenth Circuit considered a prosecution under the NSPA arising out of the alleged theft of a computer program and its source code. Although the stolen program was located at the defendant's residence, the prosecution could not prove that the software had been physically removed from plaintiff's place of business. [FN51] The intangible properties of computer programs led the court to state "for § 2314 to apply there must be some tangible item taken, however insignificant or valueless it may be, absent the intangible component." [FN52] Accordingly, the Tenth Circuit held that the "essential ingredient of the statute *908 [§ 2314]--the involvement of physical 'goods, wares, [or] merchandise' that were themselves 'stolen, converted or taken by fraud'--was missing ...." [FN53]

C. Trade Secrets Act

Prior to the EEA, the only federal statute that specifically addressed the theft of trade secrets was the Trade Secrets Act, which prohibits the unauthorized disclosure of confidential information by government employees. [FN54] Because this legislation does not apply to private sector employees, federal prosecutors more often turned to the NSPA and Mail and Wire Fraud statutes for criminal misappropriation of trade secrets. [FN55]

D. Mail and Wire Fraud Statutes

The mail and wire fraud statutes [FN56] provide criminal sanctions for using or attempting to use the mails
Violations of these statutes require neither proof that the scheme's victims were in fact defrauded, nor proof that the defendant gained anything through the scheme. Rather, violations turn on actual intent to harm the victim.

In some cases, appellate courts have upheld convictions under the mail and wire fraud statutes even when there has been no violation of the NSPA. This resulted from the statutes' broader definition of property as compared to the NSPA's definition of "goods, wares and merchandise." However, under the mail and wire fraud statutes, use of the mail or wire is necessary for there to be misappropriation. In addition, if the defendant did not permanently deprive the original owner of the use of the property through fraud, the fraud requirement of the statutes will not be met.

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"). Although many cases brought under RICO are civil actions, the predicate acts necessary to sustain a RICO claim are violations of criminal law. 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, wire fraud, activity prohibited by the NSPA, and the receipt of stolen property.

Courts faced with trade secret theft charges have reached different conclusions on the definition of a "pattern of racketeering activity" within the meaning of the RICO statute. One district court held that the definition is met by a single scheme of trade secrets misappropriation if there are sufficient allegations of concerted activity directed toward a goal of injuring the plaintiff. In this case, the plaintiff alleged that the defendant's scheme to misappropriate the plaintiff's trade secrets included multiple mailings and telephone conversations, in violation of the mail fraud and wire fraud statutes. The court held this scheme established a pattern of racketeering activity.

F. State Law Provisions

In addition to the various federal statutes criminalizing the misappropriation of trade secrets, all states have enacted criminal statutes applicable to the theft, use, or disclosure of another's trade secrets. These state statutes vary greatly in their scope and sanctions. Some specifically address trade secrets while others have been interpreted to cover trade secrets despite no explicit reference to them. However, the scope of protection afforded by some state statutes is, like the scope of the NSPA, limited because they apply only to the theft of tangible items.

III. TRADEMARK COUNTERFEITING

Over the past several decades, the theft of trademarks, the symbols or names associated with brand names and products, has become an increasingly lucrative activity for criminals. It has also had an equally significant, but opposite effect on the economy, as companies lose an estimated $200 billion a year to criminal commercial trademark counterfeiting.

This Section will cover the various statutes that the government uses to protect companies' investments in developing brand names and trademarks. Part A addresses the Trademark Counterfeiting Act of 1984, including its similarities to and differences from its civil counterpart, the Lanham Act. It also reviews defenses to charges of trademark counterfeiting and discusses the FBI's recent campaign against trademark counterfeiting. Part B covers the trademark counterfeiting provisions of the Racketeer Influenced and Corrupt Organizations Act and of the Money Laundering Act.
A. Trademark Counterfeiting Act

The Trademark Counterfeiting Act ("TCA") criminalizes the intentional trafficking in counterfeit goods or services. [FN83] Counterfeit goods include those that have a *912 mark identical to or substantially indistinguishable from a registered trademark. [FN84] The government must prove that the defendant intended to traffic in goods or services and knowingly used a counterfeit mark on or in connection with those goods, [FN85] but it need not prove that the defendant had a criminal intent. [FN86] The government may also prosecute conspiracies to violate the statute. [FN87]

1. Defenses

The TCA incorporates the defenses of its civil counterpart, the Lanham Act. [FN88] thereby ensuring that no person is found guilty of violating the criminal statute if he would not have been found liable for violating a civil trademark infringement suit. [FN89] These defense include laches, unclean hands, fraud in obtaining trademark registration, use of mark in violation of antitrust laws, and invalid trademark. [FN90]

2. Operation Counter Copy

In May 1997, the U.S. Department of Justice ("DOJ") announced the initial results of a nationwide crack-down on criminal trademark and copyright fraud-- "Operation Counter Copy"--which commenced in October 1996. [FN91] According to the DOJ, this operation netted thirty-five indictments in its first six months, including three indictments of individuals for conspiracy and trafficking in trademark infringing products. [FN92] The DOJ initiated "Operation Counter Copy" as part of its overall "increase[d] effort to address criminal violations of intellectual property rights." [FN93]

B. RICO and Money Laundering Act

As with theft of trade secrets, trademark counterfeiting is also illegal under the Racketeer Influenced and Corrupt Organizations ("RICO") and money laundering statutes. In 1994, Congress added trademark counterfeiting to the list of unlawful *913 activities under the money laundering statute. [FN94] The Anticounterfeiting Consumer Protection Act of 1996 made trademark and copyright counterfeiting a predicate offense under RICO. [FN95] Due to frustration with the usefulness of the TCA in providing remedies to trademark counterfeiting, Congress amended the RICO statute to enable the government to counter organized criminal activity as a whole "rather than merely react to each crime the organization commits." [FN96]

1. Penalties

Furthermore, penalties for violations of the RICO and money laundering statutes are significantly more severe than those under the TCA. [FN97] While the aforementioned amendments do not expand the definition of conduct that is illegal under the TCA and do not necessarily increase penalties associated with that conduct, their provisions do increase penalties when used to prosecute an organized crime. [FN98]

Under the TCA, an individual who intentionally traffics in goods or services and knowingly uses a counterfeit mark shall be fined no more than $2,000,000 or imprisoned not more than ten years, or both. [FN99] For organizations, the fine shall not be more than $5,000,000. [FN100]

Under RICO, however, fines can be significantly greater--up to twice the gross profits or other proceeds of the activity. [FN101] 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. [FN102]
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." [FN103]

At this time, there have been no reported cases decided under the RICO anticounterfeiting provisions. However, the new provisions require the Attorney General to maintain statistics for all actions related to prosecution of trafficking in counterfeit goods and services. [FN104]

**4. COPYRIGHT**

Part A discusses the Copyright Act, emphasizing the elements of the criminal copyright infringement offense and affirmative defenses and the effects of reverse engineering. Parts B through E describe the application of the National Stolen Property Act, mail and wire fraud statutes, the Racketeer Influenced and Corrupt Organizations Act, and the money laundering statute to criminal copyright infringement. Part F discusses pending legislation to extend copyright protection to Warez Sites.

A. Copyright Act

Congress' exclusive power to regulate copyright law is grounded in the Constitution. [FN105] Criminal copyright infringement, first introduced into federal copyright law in 1897, has, for exactly one century, been distinguished from civil violations by the requirement that the conduct be willful and undertaken for profit. [FN106] Since 1897, the criminal copyright statute has been frequently amended as Congress has attempted to strengthen and broaden its scope. [FN107] The Copyright Act of 1976 [FN108] relaxed the mens rea requirement for criminal copyright infringement by requiring only that the infringement be undertaken willfully and for purposes of commercial advantage or private financial gain. [FN109] This lower threshold eases the burden of proving that the transgressor acted "for profit."

In 1982, Congress increased the sanctions for criminal infringement, [FN110] codifying stricter fines for criminal infringement in a separate statute. [FN111]

Enacted by Congress in October 1992, the Copyright Felony Act [FN112] responded *45 primarily to the growing problem of large-scale computer software piracy. [FN113] Prior to its passage, only unauthorized copying of sound recordings, motion pictures, or audiovisual works was a federal felony. [FN114] The Act amended 18 U.S.C. § 2319 by broadening its coverage to protect all copyrighted works, and lowering the numerical and monetary thresholds for felony sanctions. [FN115] The mens rea requirement remained unchanged under the 1992 Act, requiring the government to prove that the infringer's conduct was both willful and for purposes of commercial advantage or private financial gain. [FN116]

Finally, on December 16, 1997, the "No Electronic Theft (NET) Act" was enacted. [FN117] This Act removes the requirement that the willful infringer have done so for financial gain; the government need only prove either that the infringer did her actions for financial gain, or that she reproduced or distributed one or more copies of copyrighted works which have a total retail value of $1,000. [FN118] Thus, the criminal copyright statute now reaches those infringers who act solely to harm another or for nonfinancial gratification. [FN119]

Because a copyright cannot exist before an expression is captured in a fixed, tangible medium, musical or dramatic performances may not be protected by copyright until they are recorded. A performer's interest in her performance is protected against unauthorized recording by 18 U.S.C. § 2319A. This section, added in December 1994, provides for both fines and imprisonment for the recording, reproduction, transmission and distribution (whether for sale or not) of *46 live musical performances. [FN120]

1. Elements of the Offense

The government has the burden of proving three elements in a criminal prosecution for copyright infringement
under 17 U.S.C. § 506: (1) that a copyright has been infringed upon; (2) that the violation was performed willfully; and (3) that the infringement was for purposes of commercial advantage or private financial gain, or that the infringer reproduced or distributed, during any 180-day period, 1 or more copies or phonorecords of one or more copyrighted works, with a total retail value of more than $1,000. [FN121] The elements of a § 2319A violation are similar. [FN122]

As in civil cases, the first element--copyright infringement--can be proven by direct evidence, if available, [FN123] or by indirect evidence showing that the defendant had access to the copyrighted work and that the alleged copy is "substantially similar" to the original work. [FN124] The substantial similarity test, which is not necessarily required, [FN125] is a two step analysis which requires: (1) 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 (2) a showing that the defendant's alleged copy expresses the same "intrinsic" substance and value as the original work. [FN126] As an alternative to the substantial similarity test, courts may employ the "virtual identity" standard, or they may apply both. Whereas the *917 substantial similarity test allows the potentially infringing work to be broken down into protectable and unprotectable elements, which will be compared with the original work for substantial similarity, the virtual identity test looks at the two works as a whole to determine if they are virtually identical. [FN127]

In McCulloch v. Albert E. Price, Inc., [FN128] the Ninth Circuit held that it is not necessary under the substantial similarity test to determine the scope of copyright protection, or to identify the idea behind a copyright holder's work. [FN129] The McCulloch court also decided that although the district court did not expressly follow the prevailing two-prong substantial similarity test, [FN130] the fact that the lower court found a "confusing" similarity of ideas and expressions among the works was sufficient to support a finding of substantial similarity. [FN131] Some courts allow the allegedly infringing work to be separated from the noninfringing work by filtering out copyright protected from non-protected components. [FN132] Finally, the copyright infringement element may be established even though the person distributing the infringing work did not produce the copies herself. [FN133]

Intent to infringe is the second element that must be established. A majority of the courts have interpreted the term "willfully" to mean that the government must show that the defendant specifically intended to violate the copyright law. [FN134] The Second and Ninth Circuits have taken the minority view, holding that "willfulness" *918 requires only an intent to copy, not an intent to infringe. [FN135]

With regard to the third element, intent to profit, the Seventh Circuit has held that a defendant need not actually realize commercial advantage or private financial gain to be convicted of copyright infringement. [FN136] It is enough that the defendant commit the violation for the purpose of financial gain. [FN137] However, the aforementioned December 1997 amendments to 17 U.S.C. § 506(a) have removed the financial gain requirement, by allowing the government to prove either financial gain, or that one or more copies were reproduced or distributed with a total retail value of more than $1,000; thus, the infringer need not have intent to profit to be found guilty. [FN138]

2. Defenses

A common statutory defense to copyright infringement is the first sale doctrine. [FN139] According to the doctrine, upon sale, the author conveys title to the particular copyrighted work and abolishes his right to restrict subsequent sales of the work. [FN140] The Third Circuit has held that infringing goods do not have to be made in the United States for the first sale doctrine to apply. [FN141] However, the Ninth *919 Circuit subsequently held that a defendant could not use the first sale doctrine as a statutory defense to copyright infringement. [FN142] The Supreme Court granted certiorari to resolve this split in the circuits, and their unanimous March 1998 opinion in Quality King Distributors, Inc. v. Lanza Research International, Inc. decisively rejected the Ninth Circuit's approach, holding that the first sale defense precluded assertions by a copyright owner that the re-importation of its goods from overseas markets constituted copyright infringement. [FN143]

Other defenses include fair use, parody and scènes à faire. Fair use considers the nature of both the infringing work and the work infringed against, as well as the purpose and economic impact of the specific use. A defense of fair use as parody [FN144] considers almost exclusively the expressive intent of the infringing work to determine if
the unique message could have been adequately conveyed through a less intrusive means. \[\text{FN145}\] A scènes à faire defense \[\text{FN146}\] relies on the fact that the infringing elements are so common or integral to the sort of work being produced that it is impossible to create works in the same category without those elements and therefore they may not be protected by copyright. \[\text{FN147}\]

**3. Reverse Engineering**

Because only the expression of an idea, and not the idea itself, may be protected under copyright, a copy made for the purposes of reverse engineering may represent a fair use exception to the copyright doctrine. Reverse engineering is the process, now most often applied to software, where a protected work is broken down to its component and nonprotected parts, from which a similar, competitive but noncopy product may be created. \[\text{FN148}\]

While this is more often at issue in trade secret violations, the doctrine has been applied to copyright violations in software cases. \[\text{FN149}\]

**B. National Stolen Property Act**

In Dowling v. United States, \[\text{FN150}\] the Supreme Court held that the interstate transportation of goods infringing on another's copyright does not fall within the scope of the National Stolen Property Act. \[\text{FN151}\] Because there had been no actual physical removal or theft of the property, the Court held that the Act's requirement that the goods be "stolen, converted or taken by fraud" was not met. The decision overruled a long line of cases extending the protection of the Act to copyrighted goods. \[\text{FN152}\]

**C. Mail and Wire Fraud Statutes**

The mail and wire fraud statutes \[\text{FN153}\] impose criminal penalties on those who utilize the mails or wires to defraud others through copyright infringement. \[\text{FN154}\] To establish a violation of either statute, the government must meet the same criteria as set out in Section II.D of this Article. Additionally, one district court has held \*921 that federal copyright law does "not necessarily preempt other proprietary rights." \[\text{FN155}\] Because the defendants in that prosecution would not profit from their infringement until transmission by wire had occurred, this court held that remedies were not limited to those provided by the copyright statute and that prosecution under the wire fraud statute was acceptable. \[\text{FN156}\]

**D. Racketeer Influenced and Corrupt Organizations Act**

As with theft of trade secrets and trademark counterfeiting, RICO \[\text{FN157}\] claims can be brought for copyright infringement 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. \[\text{FN158}\] The Anticounterfeiting Consumer Protection Act of 1996 has made copyright counterfeiting a racketeering activity under RICO. \[\text{FN159}\]

**E. Money Laundering Act**

Section 1956 of the money laundering statute defines money laundering and includes the receipt of proceeds from trafficking in counterfeit goods or goods infringing copyright as specified unlawful activities. \[\text{FN160}\]

**F. The Database Protection Bill**

In October 1997, Rep. Howard Coble (R.-N.C.) introduced the Collections of Information Antipiracy Act, \[\text{FN161}\] which would provide criminal penalties for the use of all or part of a "collection of information gathered, organized, or maintained by another person through the investment of substantial monetary or other resources." \[\text{FN162}\] A violation of the proposed law would require willful action, that the act be undertaken for commercial or
financial advantage--whether direct or indirect--and that the perpetrator cause loss or damage to the compiler of the information. [FN163] Similar legislation introduced in the 104th Congress [FN164] was *922 defeated and was criticized for extending copyright protection to hitherto uncopry-rightable databases. [FN165] Even if the current bill is not ultimately enacted, it might serve as a model for future legislation. [FN166]

V. ONLINE SERVERS: CRIMINAL VIOLATIONS OF THE COPYRIGHT FELONY ACT

Part A of this section outlines applications of the Copyright Act to on-line activities. It then addresses applications of the first-sale doctrine to file transfers in cyberspace. Part B discusses criminal liability by focusing on the dual requirements of intent and commercial advantage/financial gain. Finally, Part C addresses Warez Sites and Internet Service Providers' liability for activities on their networks.

A criminal violation of the Copyright Act occurs when one willfully reproduces or publicly distributes any kind of copyrighted work. [FN167] The Copyright Act of 1976 [FN168] protects the use of the text files, [FN169] image files, [FN170] and sound files [FN171] on the Internet. [FN172] Criminal copyright infringement that is facilitated by or achieved through the Internet and which meets the statutorily prescribed number of copies or dollar value may lead to felony prosecution. [FN173] Systematic, unauthorized *923 trading in copyrighted works on the Internet--whether sound, picture, or text files, or unlicensed software distribution--potentially qualifies as trafficking in counterfeit works. [FN174]

The protection that the 1976 Copyright Act affords digital works is a matter of dispute. [FN175] There are several areas of the Act that commentators have argued should be amended in light of the growing use of cyberspace. Two issues addressed here are the "first sale doctrine" exception and the statutory requirement that criminal liability be based on findings of intent and commercial or financial gain.

A. The Internet and the First Sale Doctrine

The first sale doctrine allows a copyright holder to legally sell or give away her copy of the work. [FN176] Literally applied to file transfers in cyberspace, the doctrine arguably implies that a person who legally downloads [FN177] a file copy to her own computer can freely redistribute that copy, whether or not she assesses a fee, to *924 anyone else. [FN178] The problem attending such cyberspace redistribution lies in the ability of the first owner to retain a copy of the file she transfers. Eventually, the argument goes, the copyrighted item will be so widely and freely available, and the demand will fall so low, that the owner will no longer benefit financially from her copyrighted work. In response, the authors of White Paper argue that the first sale doctrine should not apply to the Internet at all. [FN179] Currently, the unauthorized reproduction or public distribution of any kind of copyrighted work can result in a felony prosecution. [FN180]

B. Criminal Liability

1. The Intent Requirement

Criminal liability for copyright infringement is predicated on a finding that the alleged perpetrator acted willfully. [FN181] The cyberspace context complicates the prosecutor's job because the defendant can convincingly argue that she unknowingly contributed to or committed the offense. [FN182] The expansion of copyright law to address the Internet has yielded civil cases involving allegations of copyright infringement directed against the system operator ("Sysop") [FN183] or the bulletin board service ("BBS"). [FN184] Although the criminal section of the Copyright Act *925 does not immunize on-line providers from criminal liability for either direct [FN185] or contributory copyright infringement, [FN186] to date there have been no successful criminal copyright prosecutions of system providers.

The most heated debate involving service provider liability surrounds the civil offense. Because civil liability does not require that the provider willfully intended to commit or contribute to the infringement, the question arises whether an entity that may only maintain the network should be held liable. [FN187] In Religious Technology
Center v. Netcom On-Line Communication Service, Inc., [FN188] the court held that a BBS service provider could not be held directly or vicariously liable for civil copyright infringement committed by a subscriber. [FN189] The Netcom court reasoned that, although copyright infringement is governed by strict liability, implicating a server irrespective of any intervention on its part would lead to unreasonable liability. [FN190]

2. The Commercial Advantage/Financial Gain Requirement

The "commercial advantage" or "financial gain" requirement for a finding of criminal copyright liability has hitherto hindered prosecutors. [FN191] The leading case demonstrating this problem is United States v. LaMacchia. [FN192] Even though defendant David LaMacchia set up a secret bulletin board and distributed unauthorized copies of commercially published, copyrighted software, he escaped criminal liability because he neither sought nor received financial or commercial gain from his actions. [FN193]

The Working Group, which stated that it supports amendments to the copyright law, proposed the Criminal Copyright Improvement Act of 1995 in a bill that the *926 104th Congress did not enact. [FN194] However, in 1997 Congress enacted the aforementioned No Electronic Theft (NET) Act, which expressly amended 17 U.S.C. § 506(a) to provide that the government can prove either financial gain or that one or more copies or phonorecords of one or more copyrighted works were reproduced or distributed during any 180-day period, provided that the copies have a total retail value exceeding $1,000. [FN195] This legislation also changed the statute of limitations from three years to five years, thus broadening the scope of its protection. [FN196]

C. Warez Sites and Internet Service Provider Liability

Warez Sites are anonymous, often short-lived file-transfer protocol ("FTP") sites which exist solely to disseminate unlicensed copies of software and/or passwords for pirate software. [FN197] Warez sites may be unauthorized use of server space but are not usually maintained for profit or malicious purposes. [FN198] Any user of the Internet, Usenet or a BBS and who is able to log on before all available lines are occupied can download a full, unencrypted, and unlicensed version of new software.

At the December 1996 Geneva meeting of the World Intellectual Property Organization ("WIPO"), draft treaty provisions creating liability for ISPs and Sysops were almost unanimously rejected. [FN199] Partly in response to the debate over those provisions, and partly in response to Netcom, [FN200] Rep. Howard Coble (R-N.C.) and Rep. Henry Hyde (R-Ill.) introduced the On-line Copyright Liability Limitation Act. This bill was intended to protect ISPs and Sysops from "vicarious liability relating to material on-line" if such persons merely provide the server space for the infringing material and neither control nor endorse the infringing material. [FN201] This bill would additionally protect the ISP or Sysop from liability claims seeking damages for the removal or blocking of potentially infringing sites, *927 whether or not those sites are found to violate copyright. [FN202] Unlike the rejected provisions of the WIPO Treaty, which would have required ISPs to remove, block, or report infringing sites, thus creating an impossible task for site-providers, this bill would not mandate direct action on the part of ISPs. The ISP would only have to demonstrate that it did not create, control, or endorse the site. [FN203] While the ISP must demonstrate that it did not profit directly from the dissemination of the infringing material, the fact that the ISP received payment for the disk-space used to create the site would not create liability. [FN204]

No floor actions were taken in 1997 on this bill, which was the subject of hearings before the Subcommittee on Courts and Intellectual Property. [FN205] Although the bill was designed with pirate software in mind, [FN206] the language is broad enough to cover sites which contain copyrighted photographs and sound recordings.

VI. PATENT

This section is divided into three parts. Part A discusses criminal liability for false patent marking. Part B addresses counterfeiting and forging of letters patent. Finally, Part C applies the National Stolen Property Act to patent infringement.
A. False Marking

While most federal remedies for patent misuse are civil, the Patent Act [FN207] does establish criminal liability for infringement. [FN208] The D.C. Circuit has held that *928 while penal in nature, 35 U.S.C. § 292 is not a criminal statute. [FN209] False marking, however, can be a criminal offense and may be manifested in several ways by using: (1) the name or any imitation of the name of the patentee; (2) the patent number; or (3) the words "patent" or "patentee." [FN210] Additionally, the use of the word "patent," or any word or number indicating that the item is patented, in connection with an unpatented 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. [FN211] In order to prove any of the above violations, deceitful intent of the defendant must be shown. [FN212]

B. Counterfeiting or Forging Letters Patent

Letters Patent are the display of information, on the item, that the government has given the manufacturer the right to exclude others from making that item. The Letters Patent statute [FN213] imposes criminal sanctions on persons forging, counterfeiting or altering any letters patent, as well as knowingly passing, uttering, or publishing as genuine, any such letters patent. [FN214]

C. National Stolen Property Act

In addition to excluding interstate transportation of goods infringing on another's copyright from the coverage of the National Stolen Property Act, [FN215] Dowling v. United States [FN216] implied, and has been interpreted to mean, that the Act also does not apply to the interstate transportation of goods infringing on patents. [FN217] Since patent infringement, like copyright infringement, does not involve a physical taking, the Supreme Court took a literal view of the Act's requirement that the copyrighted goods in dispute be "stolen, converted or taken by fraud." [FN218]

*929 VII. ART CRIMES

Over the past few decades, art crime [FN219] has become a multi-billion dollar industry; [FN220] in some estimates, it is third only to the illegal drug smuggling and arms trading markets. [FN221] Crimes involving art range from simple theft and vandalism [FN222] to forgery, [FN223] money laundering, [FN224] and various forms of fraud. [FN225] An area of art crime that has transformed the theft of stolen art works into white collar crime is the ongoing matter of art works stolen by soldiers during or after World War II and subsequently placed on the art market. [FN226]

*930 White collar art criminals may double as art gallery or auction house dealers, museum directors or curators, [FN227] collectors, or even highly talented forgers. In some cases, even the artist may be engaged in tactics which facilitate subsequent white collar crime. [FN228] Finally, an appraiser may refuse to authenticate a legitimate art work as part of a conspiracy to drive up the value of the remaining stock. [FN229] These perpetrators use their positions of power or privilege to commit non-violent *931 crimes which often require an advanced level of education and intellect. [FN230]

Obstacles to detection, [FN231] as well as the ease with which many art crimes can be perpetrated, [FN232] contribute to the difficulty of prosecuting art crimes. The problem is *932 exacerbated by a paucity of effective legislation available to prosecutors. [FN233] However, some existing laws have met with limited success in combating art crimes; the remainder of this Section examines such approaches at the state and federal level.

Part A addresses the federal measures that have been applied to art crime prosecutions, specifically the theft of major artwork act, along with the mail and wire fraud statutes, the Copyright Felony Act, and legislation implementing an international cultural property convention. Part B reviews state approaches to prosecuting art crimes utilizing criminal simulation statutes, which adapt existing forgery laws to apply to art crimes.
A. Federal Statutes

1. Theft of Major Artwork Act

As part of the "Violent Crime Control and Law Enforcement Act of 1994," Congress enacted new statutory sections which federalized the theft of major artworks. [FN234] To fall within the scope of this statute, the defendant must either have stolen or fraudulently obtained from a museum "any object of cultural heritage," [FN235] or have received such a stolen object, knowing that it was stolen or obtained by fraud. [FN236] Additionally, the statute of limitations for returning an indictment or filing an information is set at a full 20 years after commission of the art theft, which reflects the long time period that frequently ensues between the theft and the defendant's arrest. [FN237] The first reported charge under this statute occurred in January 1998, when the FBI in Philadelphia charged two defendants *933 for allegedly stealing some 200 relics from the Historical Society of Pennsylvania. [FN238]

2. Mail and Wire Fraud Statutes

The mail and wire fraud statutes [FN239] have been used with varying degrees of success in art crime prosecutions. United States v. Center Art Gallery-Hawaii [FN240] is an example of a successful criminal prosecution using the mail and wire fraud statutes. [FN241] Cited as the culmination of the largest art fraud scandal in history, [FN242] this case resulted in convictions of the gallery's two owners and the gallery itself under the mail and wire fraud statutes. [FN243] In making its case against the defendants, the government did not focus directly on the defendants' actual sale of the forged works of art or their false appraisals, but based its case on the mailing of false authentication certificates to customers and soliciting further business over the telephone. [FN244] In United States v. Burke, [FN245] the four defendants were owners and representatives of Manhattan's Barclay Gallery and the perpetrators of a major forgery scandal. The defendants "allegedly used high-pressure telephone sales pitches" to perpetrate their scheme and were each charged with twenty-two counts of mail fraud and twenty-eight counts of wire fraud. [FN246] Each of the four defendants was convicted on all counts. [FN247]

*934 Despite these and other successful prosecutions, [FN248] several difficulties exist when applying the mail and wire fraud statutes. The mens rea requirement is a serious hurdle, requiring a showing of criminal intent for successful prosecution under the mail and wire fraud statutes. [FN249]

3. Copyright Felony Act

At first glance, the copyright laws appear to be an effective prosecutorial tool. Again, however, a stringent mens rea requirement limits their usefulness and success. Furthermore, the Copyright Felony Act only protects unpublished works and works not in the public domain, leaving many older works unprotected. [FN250] Finally, many forgeries do not involve copying. [FN251]

4. UNESCO and UNIDROIT: Enforcement by Treaties

In 1970, the United Nations Educational, Scientific, and Cultural Organization ("UNESCO") adopted the "Convention on Cultural Property Implementation" [FN252] which was ratified by the United States in 1983. [FN253] The purpose of this treaty is to protect the "cultural patrimony" of countries "from the pillage of archaeological or ethnological materials" by providing import restrictions for such objects. [FN254] The United States established the "Cultural Property Advisory Committee," [FN255] which has led to restrictions on imports of antiquities from several countries. [FN256]

*935 However, because some countries considered major forces in the art trade had failed to ratify the 1970 UNESCO Convention, UNESCO asked UNIDROIT (the International Institute for the Unification of Private Law, Rome) to prepare a new treaty that would provide protection to art trade in the rest of the world. [FN257] This
treaty, completed on June 24, 1995, would greatly expand the protection, but with one significant restriction: it only applies to art works stolen or looted after the date that the host country has ratified the treaty. [FN258] Thus far, out of the twenty-two countries who have signed the treaty, only three have ratified it, while two others have acceded to it. [FN259] The United States abstained from voting on the treaty and has not yet signed, let alone ratified, the UNIDROIT convention. Nonetheless, this convention has generated significant controversy in the United States and the United Kingdom, as art dealers claim that they will no longer be able to exhibit or sell works in countries which have ratified the convention, on the grounds that the works might be confiscated by the country of origin, leaving the U.S. art dealers without a cause of action. [FN260]

B. State Approaches

Recently, various states have recognized the importance of promoting the arts by including provisions aimed at their protection and encouraging their development. [FN261] A number of states have enacted criminal simulation statutes, designed to customize existing forgery laws which, without such modification, are limited to actions associated with written documents and checks. For example, New York's Criminal Simulation Statute [FN262] extended New York's preexisting statute aimed at forgery of cultural property to "antiques, objets d'art, rare books and comparable matter." [FN264]

Twenty-six other states and Guam have codified similar "criminal simulation provisions into their penal codes, reflecting a growing awareness of the special type of protection needed in the art community. In three states, however, these statutes do not apply to all art and antiquities, but are limited to certain excavated or historical objects. [FN266] Imposing stricter requirements, two states require disclosure of the number of copies in limited editions of fine art works, with penalties and injunctions for inadequate or erroneous disclosure. [FN267] In addition, states often use traditional statutes, such as conspiracy [FN268] or grand larceny, to prosecute art-related fraud. [FN269]

VIII. SENTENCING

Several provisions of the Federal Sentencing Guidelines are applicable to the theft of intellectual property. [FN270] This Section delineates the provisions applicable to each statute, beginning with the Economic Espionage Act and followed by the National Stolen Property Act, the Trade Secrets Act, the mail and wire fraud statutes, the RICO Act, the Trademark Counterfeiting Act and Copyright Felony Act, and False Marking and Counterfeiting or Forging Letters Patent. Since a defendant may be prosecuted under any combination of these statutes, the grouping analysis will be important in determining the defendant's sentence after a multi-count conviction. [FN271]

A. Economic Espionage Act of 1996

Defendants who are convicted of violating 18 U.S.C. § 1831 can be imprisoned for a maximum of fifteen years and fined $500,000 or both. [FN272] Those convicted of violating § 1832 can be imprisoned for up to ten years and fined $500,000. [FN273] Furthermore, the Economic Espionage Act provides a mandatory forfeiture of any proceeds or property derived from violations of the Act, but leaves to the court's discretion the option to order the forfeiture of any property used to commit or facilitate the commission of the crime. [FN274] Existing remedies are still available under state law; the Act specifically states that it does not "preempt or displace any other remedies, whether civil or criminal." [FN275]

B. National Stolen Property Act

The penalty for violations of the National Stolen Property Act [FN276] is imprisonment for not more than ten years, a fine determined under Title 18, or both. [FN277]

Defendants convicted of violating the Act are sentenced under § 2B1.1. [FN278] The base offense level of four is based upon a total loss to the victim of $100. [FN279] The offense level is raised as the financial loss to the
victim increases, up to a maximum increase of twenty offense levels for a loss exceeding $80,000,000. [FN280] Additionally, if the offense involved more than minimal planning, the offense level is increased by two levels. [FN281] Finally, if the defendant is a person in the business of receiving and selling stolen property, the offense level is increased by four levels. [FN282]

C. Trade Secrets Act

Violators of the Trade Secrets Act [FN283] may be fined under Title 18 and imprisoned *939 for up to one year; moreover, violators shall be removed from office or employment. [FN284] Violators are sentenced under § 2H3.1. [FN285] The base offense level is nine and is increased by three levels if the purpose of the conduct was to obtain commercial advantage or economic gain. [FN286] However, if the purpose of the conduct was to facilitate another offense, § 2H3.1 requires the application of the guideline applicable to an attempt to commit that offense, provided that the resulting offense level is greater than that determined under § 2H3.1. [FN287]

D. Mail and Wire Fraud Statutes

Violators of either statute, mail or wire fraud, [FN288] are subject to a fine determined under Title 18, not more than five years of imprisonment, or both. [FN289] If the violation affects a financial institution, the defendant may be fined up to $1,000,000 or imprisoned for not more than thirty years, or both. [FN290]

Defendants convicted of mail or wire fraud are sentenced under § 2F1.1, "Offenses Involving Fraud or Deceit." [FN291] The base offense level of six is based upon a total loss to the victim of $2,000 or less. [FN292] The offense level is raised as the financial loss to the victim increases, up to a maximum increase of eighteen offense levels for fraud of over $80,000,000. [FN293] Additionally, the offense level can be raised for a number of reasons, including: an increase of two levels if the crime involved more than one victim, or if the crime involved more than minimal planning. [FN294]

E. Racketeer Influenced and Corrupt Organizations Act

Violation of RICO carries a fine determined under Title 18, not more than *940 twenty years imprisonment, or both. [FN295] Additionally, it requires that the defendant forfeit his interest in any enterprise established, operated, or maintained in violation of the statute. [FN296] Defendants convicted of RICO violations are sentenced under § 2E1.1. [FN297]

The Anticounterfeiting Consumer Protection Act of 1996 broadens the scope of RICO to include intellectual property violations but does not change the penalties. [FN298]

F. Trademark Counterfeiting Act and Copyright Felony Act

Individuals convicted of trafficking in forged or counterfeit goods face a fine of up to $2,000,000, not more than ten years imprisonment, or both. [FN299] Similarly, organizations convicted of trafficking in counterfeit goods face a fine of up to $5,000,000. [FN300] Additionally, upon a determination that any articles in the possession of a defendant bear counterfeit marks, the United States may obtain an order for the destruction of the goods. [FN301]

First time offenders convicted of trafficking goods that bear forged or counterfeited labels face a fine determined under Title 18, not more than five years' imprisonment, or both. [FN302]

The Copyright Felony Act states that a felony offense consists of the reproduction or distribution, during any 180-day period, of at least ten unauthorized copies, of one or more copyrighted works, with a collective value of more than $2,500. [FN303] First-time offenders may be imprisoned for not more than five years, [FN304] or fined not more than $250,000 for an individual, or $500,000 for an organization; [FN305] *941 individuals may be both fined and imprisoned. [FN306] In addition, if the offender derives personal financial gain from the offense, or
causes financial loss to another, the offender may be fined up to the greater of twice the gross gain or twice the gross loss. \[\text{FN307}\] If the offender has been previously convicted under the statute, the maximum prison sentence increases to not more than ten years, and the repeat offender also may be subject to the $250,000 fine. \[\text{FN308}\] Moreover, the Copyright Felony Act prescribes a misdemeanor sentence of not more than $100,000 fine and a maximum of one year imprisonment for any criminal copyright infringement failing to meet the numerical thresholds described above. \[\text{FN309}\] Finally, § 506(b) gives courts the discretion to order the forfeiture and destruction of infringing items and all implements, devices, or equipment used in their manufacture. \[\text{FN310}\]

Similarly, violators of § 2319A can be imprisoned for not more than five years, fined under Title 18, or both. \[\text{FN311}\] For second or subsequent offenses, violators can receive prison sentences of ten years, a fine under Title 18, or both penalties. \[\text{FN312}\] The violator of this statute surrenders his right to the illegal material. \[\text{FN313}\]

Defendants convicted of trademark counterfeiting \[\text{FN314}\] or criminal copyright infringement \[\text{FN315}\] are sentenced under § 2B5.3. \[\text{FN316}\] The base offense level is six. \[\text{FN317}\] If the retail value of the infringing items exceeds $2,000, then the offense level is increased by the corresponding number of levels from the table in § 2F1.1 (Fraud and Deceit). \[\text{FN318}\] However, the reference in § 2B5.1 to the table contained in § 2F1.1 applies only to the actual table, not to the entire offense guideline, which means that enhancements contained in § 2F1.1 are not applicable to defendants convicted of violating § 2319 or § 2320. \[\text{FN319}\]

*942 G. False Marking and Counterfeiting or Forging Letters Patent

False marking violations under § 292 result in fines of up to $500 per offense. \[\text{FN320}\] Moreover, each false marking is subject to a separate fine. \[\text{FN321}\] Half of the proceeds from a § 292 conviction go to the citizen who brings the crime to the attention of the government; the other half of the proceeds go to the United States. \[\text{FN322}\]

Violators of the Letters Patent statute \[\text{FN323}\] face fines pursuant to § 3571 of Title 18. \[\text{FN324}\] not more than ten years imprisonment, or both. \[\text{FN325}\] Defendants convicted of counterfeiting or forging letters patent are sentenced under § 2F1.1. \[\text{FN326}\]

[FNa1]. The authors and editors gratefully acknowledge the review provided by Peter J. Toren (Computer Crime and Intellectual Property Section, Criminal Division, Dep’t of Justice) of the 1997 INTELLECTUAL PROPERTY CRIMES Article, which was most helpful in researching and updating this year’s Article. This review represented his own comments, and does not embody the views of the Department of Justice.

[FN1]. Traditionally, theft of trade secrets has been handled by civil remedy. However, because of increased technological complexity, delays in civil litigation, and advances in computer technology, all of which permit thieves to profit more rapidly from trade secrets, traditional remedies, such as injunctions and civil damages, have become ineffective. Furthermore, because of the intangible nature of trade secrets, which once lost can never be physically recovered, the civil remedy is quite illusory.


secret property rights).


[FN5]. 18 U.S.C.A. § 1832 (Supp. 1998). The EEA provides for a maximum term of imprisonment of fifteen years if the criminal act was done with the intent to benefit a foreign government and ten years in all other cases. The maximum fine that may be imposed upon an organization is $10 million if the intent of the organization was to benefit a foreign government. In all other cases, the maximum fine imposed on an organization is $5 million. 18 U.S.C.A. §§ 1831-1832 (Supp. 1998).

[FN6]. 18 U.S.C.A. § 1839 (Supp. 1998). Even if the original owner never loses custody over his property, the EEA recognizes the loss of value to that owner. COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, U.S. DEPT OF JUSTICE, FEDERAL PROSECUTION OF VIOLATIONS OF INTELLECTUAL PROPERTY RIGHTS (COPYRIGHTS, TRADEMARKS AND TRADE SECRETS) 73 (1997) [hereinafter "FEDERAL PROSECUTION MANUAL"]').


[FN9]. Id.

[FN10]. FEDERAL PROSECUTION MANUAL, supra note 6, at 75.

[FN11]. Section 1832 states in relevant part:

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....

18 U.S.C.A. § 1832(a) (Supp. 1998). The five clauses of §§ 1831(a) and 1832(a) are presumably disjunctive so that violation of any one clause is sufficient to violate the statute. 18 U.S.C.A. §§ 1831(a), 1832(a) (Supp. 1998).


[FN15]. 18 U.S.C.A. § 1832(a)(3) (Supp. 1998); see also Pooley, supra note 14, at 192 (stating that EEA provisions are in some respects significantly broader than other civil trade secret laws).


[FN19]. Section 1833 states:

This chapter does not prohibit--

(1) any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State; or

(2) the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.


[FN21]. Id.


[FN23]. Pooley, supra note 14, at 189.

[FN24]. EEA HOUSE REPORT, supra note 20, at 7.


[FN27]. FBI Charges, supra note 26, at 12,413.


[FN29]. Id.


[FN32]. Id. Section 2314 goes on to provide criminal sanctions to any person:

having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transports or causes to be transported, or induces any person or persons to travel in, or to be transported in interstate or foreign commerce in the execution or concealment of a scheme or artifice to defraud that person or those persons of money or property having a value of $5,000 or more .... 18 U.S.C. §  2314 (1994).

[FN33]. See United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988) (finding theft of sample of synthetic casting material used in repairing broken bones falls under NSPA even though a major portion of its value comes from an intangible component); United States v. Bottone, 365 F.2d 389, 393-94 (2d Cir. 1966) (holding NSPA applicable to theft of documents containing trade secrets); United States v. Seagraves, 265 F.2d 876, 880 (3d Cir. 1959) (finding theft of geophysical maps identifying possible oil deposits to fall under NSPA).


[FN35]. See United States v. Brown, 925 F.2d 1301, 1305 (10th Cir. 1991) (dismissing prosecution because could not prove that computer program physically removed from plaintiff's place of business); Abbott v. United States, 239 F.2d 310, 312 (5th Cir. 1956) (requiring government to prove "[w]ho carried it, or how, or who caused it to be transported"); see also Bottone, 365 F.2d at 393 (finding that NSPA covers photocopies transported in interstate commerce stolen from company and not made on company's equipment); Howington, 623 F. Supp. at 1558 (holding plaintiff failed to allege transportation by "merely stat[ing] that a trade secret was appropriated in violation of the statutes").

[FN36]. 265 F.2d 876 (3d Cir. 1959). In Seagraves, the stolen trade secrets were geophysical and geological maps produced by Gulf Oil and copied with its equipment onto its paper. The court distinguished the instant case from others by noting that the trade secrets stolen were "the permanent form into which was cast the advice and assistance for which the defendants were consulted." Id. at 880. Evidence showed that maps of this type were frequently sold. In addition, expert testimony established the value of some of the individual maps at well over $5,000. Id.; see Brown, 925 F.2d at 1308-09 (placing a restriction that goods, wares or merchandise must be transported in physical form to qualify as stolen trade secrets under NSPA); see also United States v. Greenwald, 479 F.2d 320, 321 (6th Cir. 1973) (finding documents containing chemical formulation to be goods, wares, or merchandise, because they were treated as assets in chemical manufacturers' market).

[FN37]. Seagraves, 265 F.2d at 880 (citing BLACK'S LAW DICTIONARY 823 (4th ed. 1951)).

[FN38]. Id.; see also Greenwald, 479 F.2d at 322 (finding established market among chemical competitors for chemical formulations sufficient to make stolen chemical formula a "good" within meaning of NSPA). But see Brown, 925 F.2d at 1308-09 (finding that computer programs are intangible intellectual property, not "goods, wares or merchandise" within meaning of NSPA). For further discussion of this topic, see the COMPUTER CRIMES article in this issue.
[FN39] See *United States v. Lyons*, 992 F.2d 1029, 1033 (10th Cir. 1993) (holding computer software stolen in conjunction with computer hardware was theft of tangible property).


[FN42] *United States v. Seagraves*, 265 F.2d 876, 880 (3d Cir. 1959); see also *United States v. Greenwald*, 479 F.2d 320, 321 (6th Cir. 1973) (attributing defendant's profits from sale of stolen chemical formulas to established market of finished products among competitors in industry). But see *In re Vericker*, 446 F.2d 244, 248 (2d Cir. 1971) (refusing to find market for papers showing that individuals are or may have been engaged in criminal activity or what procedures are used by FBI in tracking them down); *United States v. Willette*, 764 F. Supp. 759, 761-62 (N.D.N.Y. 1991) (refusing to determine value based on retail price when owner was part of wholesale market).


[FN44] *Wilson*, 900 F.2d at 1355-56 (looking to development costs and price for which defendant sold stolen goods to determine valuation absent actual market).

[FN45] *United States v. Jackson*, 576 F.2d 749, 757 (8th Cir. 1978) (using "thieves' market value" since value of contraband was speculative or not fixed and thieves' market was only guidepost available for establishing value).


[FN47] 18 U.S.C. § 2314 (1994) ("[w]hoever transports ... goods, wares, merchandise ... knowing the same to have been stolen ....") (emphasis added).

[FN48] *United States v. Bottone*, 365 F.2d 389, 392-93 (2d Cir. 1966) (holding proof of defendant's comings and goings clearly sufficient to suggest that he knew he was selling stolen goods).


[FN50] 925 F.2d 1301, 1302 (10th Cir. 1991).

[FN51] Id. at 1305.
The court explained:

[S]ection 2314 applies only to physical "goods, wares or merchandise." Purely intellectual property is not within this category. It can be represented physically, such as through writing on a page, but the underlying, intellectual property itself, remains intangible. It is true that the intellectual property involved in the instant case was more nearly "stolen, converted or taken by fraud" in the sense that it was at no time freely presented to the public .... We hold that the computer program itself is an intangible intellectual property, and as such, it alone cannot [sic] constitute goods, [or] wares ... which have been stolen, converted or taken within the meaning of § 2314 or § 2315.

Id. at 1307-08 (citations omitted).

Cf. United States v. Lyons, 992 F.2d 1029, 1033 (10th Cir. 1993) (clarifying Brown by allowing sentencing under NSPA because defendant stole both software and hardware) (emphasis added).


There is only one reported decision under this statute, United States v. Wallington, 889 F.2d 573 (5th Cir. 1989). Id. at 179 n.5. Since the statute only provides for misdemeanor sanctions, it has not often been used to prosecute unauthorized disclosures. Id.

The mail fraud statute is flexible since almost any use of the mail brings one under the statute's prohibitions. See Schmuck v. United States, 489 U.S. 705, 710-11 (1989) (holding that use of mail need not be essential part of the scheme but only a "step in [the] plot").

For a more extensive discussion of the mail and wire fraud statutes, see the MAIL AND WIRE FRAUD article in this issue.

See United States v. Henry, 29 F.3d 112, 114 (3d Cir. 1994) (stating "[t]he statutes cover schemes to defraud another of intangible property, such as confidential business information").

See United States v. Dixon, 536 F.2d 1388, 1399 n.11 (2d Cir. 1976) (requiring prosecution to prove "some actual harm or injury was contemplated"); see also United States v. Von Barta, 635 F.2d 999, 1006 (2d Cir. 1980) (stating defendant must have intended to defraud), overruled on other grounds by Ingber v. Enzor, 841 F.2d 480 (2d Cir. 1988); United States v. Regent Office Supply Co., 421 F.2d 1174, 1181 (2d Cir. 1970) (stating that there must
be showing of intended harm; misrepresentations amounting to deceit are not sufficient to constitute fraudulent intent).

[FN64]. FEDERAL PROSECUTION MANUAL, supra note 6, at 91-92; see also Abbott v. United States, 239 F.2d 310, 315 (5th Cir. 1956).

[FN65]. FEDERAL PROSECUTION MANUAL, supra note 6, at 92.


[FN67]. Id.


[FN69]. See Religious Tech. Ctr. v. Wollersheim, 796 F.2d 1076, 1077 (9th Cir. 1986) (recognizing civil RICO claims for trade secret theft; finding that injunctive relief not available in this RICO action).


[FN76]. Id.

[FN77]. Id. at 375. But see Fleet Mgmt. Sys., Inc. v. Archer-Daniels- Midland Co., 627 F. Supp. 550, 559 (C.D. Ill. 1986) (holding isolated criminal episode, though accomplished through several fraudulent acts, does not evidence "threat of continuing criminal activity" so as to give rise to pattern of racketeering activity within meaning of RICO). The suit alleged that the defendant had misappropriated computer software it had obtained by license from the plaintiff and then fraudulently misrepresented to plaintiff that it had purged the software from its computer system in numerous mail and wire communications over the next two years. Id. at 552-53; see also H.J. Inc. v. Northwestern Bell Tel. Co., 492 U.S. 229, 239 (1989) (stating at least two separate predicate acts of racketeering activity that have continuity and relationship and pose threat of continued criminal activity are required to prove pattern of racketeering activity).


"Anticounterfeiting House Report".


[FN85]. 18 U.S.C. § 2320(a) (1994); see also United States v. Hon, 904 F.2d 803, 805-807 (2d Cir. 1990) (presenting requirements for prosecuting criminal trademark counterfeiting offense); United States v. Infurnari, 647 F. Supp. 57, 59-60 (W.D.N.Y. 1986) (explaining the requirement that the counterfeit mark can be likely to cause confusion among immediate purchasers or prospective purchasers).

[FN86]. See United States v. Baker, 807 F.2d 427, 429 (5th Cir. 1986) (relying on legislative history to show that criminal intent is not required).

[FN87]. FEDERAL PROSECUTION MANUAL, supra note 6, at 56.


[FN89]. 18 U.S.C. § 2320(c) (1994); see also FEDERAL PROSECUTION MANUAL, supra note 6, at 59.

[FN90]. FEDERAL PROSECUTION MANUAL, supra note 6, at 59.

[FN91]. United States Dep't of Justice, FBI Releases First Results of Nationwide Crack Down on Criminal Trademark and Copyright Fraud (last modified May 8, 1997) <http://www.usdoj.gov/criminal/cybercrime/195_ag.html>.

[FN92]. Id.

[FN93]. Id.


[FN96]. ANTICOUNTERFEITING HOUSE REPORT, supra note 82, at 3-4 (1996).

[FN97]. FEDERAL PROSECUTION MANUAL, supra note 6, at 61.

[FN98]. ANTICOUNTERFEITING HOUSE REPORT, supra note 82, at 6.

[FN100]. Id. Repeat offenders, whether individuals or organizations, will receive harsher penalties. Id.


[FN103]. ANTICOUNTERFEITING HOUSE REPORT, supra note 82, at 7.


[FN105]. U.S. Const. art. I, § 8, cl. 8. Congress shall have the power "[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." Id.


[FN107]. See LaMacchia, 871 F. Supp. at 539-40 (discussing history of criminal copyright law); FEDERAL PROSECUTION MANUAL, supra note 6, at 17-39 (describing the criminal copyright statute); Mary Jane Saunders, Criminal Copyright Infringement and the Copyright Felony Act, 71 DENV. U. L. REV. 671, 673-75 (1994) (same).


[FN111]. 18 U.S.C. § 2319 (1994). While certain acts of criminal copyright infringement were defined as felonies, most infringements remained misdemeanor offenses. Id.
For an in-depth discussion of the legislative history of the Copyright Felony Act, see Saunders, supra note 107, at 679-80.

For a discussion of what constitutes copyright infringement of computer software, see MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 518-19 (9th Cir. 1993), which found that "copying" occurs even when a copyrighted program is temporarily loaded into a computer's RAM (random access memory). See also Religious Tech. Ctr. v. Netcom On-line Communication Serv., Inc., 907 F. Supp. 1361, 1368-73 (N.D. Cal. 1995) (holding Internet provider not liable for copyrighted material loaded onto computer by third party when provider lacked knowledge that material was copyrighted). Although there is a statutory provision, 47 U.S.C.A. § 230(c)(1) (Supp. 1998), which protects Internet providers from being considered as authors of allegedly defamatory materials posted by third parties, this provision does not extend to intellectual property rights. See 47 U.S.C.A. § 230(d)(2) (Supp. 1998) (stating that "nothing in this section shall be construed to limit or expand any law pertaining to intellectual property"); see also Zeran v. America Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997) (holding that Section 230 of the Communications Act of 1996 "plainly immunizes computer service providers like AOL from liability for [allegedly defamatory] information that originates with third parties").


Under the 1992 Act, felony sanctions applied to ten or more copies made within a 180 day period, with a retail value more than $2,500. Id.

The section also provides for forfeiture, seizure and destruction of such unauthorized recordings, and encompasses the distribution in the United States of copies of unauthorized recordings made outside the United States. 18 U.S.C. § 2319A(b)-(c) (1994).
described in paragraph (1), regardless of whether the fixations occurred in the United States....
Id; see also FEDERAL PROSECUTION MANUAL, supra note 6, at 40.

[FN123]. See United States v. Larracuente, 952 F.2d 672, 673 (2d Cir. 1992) (discussing infringement element of
prima facie case).

[FN124]. See United States v. Cohen, 946 F.2d 430 (6th Cir. 1991) (upholding a conviction of criminal copyright
infringement supported by circumstantial evidence); Saunders, supra note 107, at 682-85.

[FN125]. See McCulloch v. Albert E. Price, Inc, 823 F.2d 316, 319 (9th Cir. 1987) (holding that trial court's finding
that two objects were "confusingly similar in appearance" was tantamount to finding of substantial similarity even
without express application of two prong test).

[FN126]. See Sid & Marty Krofft Television Prod., Inc. v. McDonald's Corp., 562 F.2d 1157, 1164 (9th Cir. 1977)
(differentiating extrinsic and intrinsic prongs of substantial similarity test).

[FN127]. For a comparison of the virtual identity and substantial similarity tests for infringement, see Apple
Computer, Inc. v. Microsoft Corp., 35 F.3d 1435 (9th Cir. 1994). Virtual identity may be a more useful standard for
determining infringement in the case of "reverse engineering," whereby programmers dissect legally obtained
software and then instruct a third set of programmers on functional requirements of the software, thus creating
"virtually identical" software programs which are not exact copies of one another.

[FN128], 823 F.2d 316 (9th Cir. 1987).

[FN129], Id. at 319.

[FN130]. See Hartman v. Hallmark Cards, Inc., 833 F.2d 117, 120 (8th Cir. 1987) (applying two-prong test to
copyrighted graphics); Cooling Sys. & Flexibles v. Stuart Radiator, Inc., 777 F.2d 485, 493 (9th Cir. 1985)
(explaining that extrinsic test can be decided as matter of law, while intrinsic test is a question of fact). See generally
Saunders, supra note 107, at 499 (discussing approaches by various courts to showing of extrinsic and intrinsic
similarities of original work and alleged copy).

[FN131], McCulloch, 823 F.2d at 319.

[FN132]. See Apple Computer, 35 F.3d at 1441-47 (describing court's proper dissection of the Microsoft graphical
user interface (GUI) into protectable and unprotectable components for purposes of evaluating substantial
similarity); Lotus Dev. Corp. v. Paperback Software Int'l, 740 F. Supp. 37, 67 (D. Mass. 1990) (stating that only
those components that are copyrightable should be analyzed). But see Atari Games Corp. v. Oman, 888 F.2d 878,
882 (D.C. Cir. 1989) (declaring that sequence of frames in computer game must be analyzed as a whole and not on a
component-by-component basis).

[FN133]. See United States v. Moore, 604 F.2d 1228, 1235 (9th Cir. 1979) (holding that government may establish
criminal infringement by proving that defendants distributed copyrighted sound recordings; it is not necessary to
prove defendants both reproduced and distributed infringing recordings).
[FN134]. Saunders, supra note 107, at 688; see also United States v. Morison, 844 F.2d 1057, 1071 (4th Cir. 1988) (establishing willful to mean that defendant knowingly did an illegal act); United States v. Cross, 816 F.2d 297, 303 (7th Cir. 1987) (holding that defendant must act with the knowledge that his activity is illegal); United States v. Heilman, 614 F.2d 1133, 1137 (7th Cir. 1980) (finding willful infringement of copyright when defendant knew material was copyrighted); cf. United States v. Manzer, 69 F.3d 222, 226 (8th Cir. 1995) (declaring that government need only prove intent to defraud, and not intent to break the law, but must go beyond proof of merely intent to copy).

[FN135]. Saunders, supra note 107, at 688; see United States v. Hernandez, 952 F.2d 1110 (9th Cir. 1991) (deciding that defendant had requisite intent to join conspiracy to infringe because he had control over tapes, had shown others how to duplicate tapes, and had transported tapes from production site to storage unit); United States v. Backer, 134 F.2d 533 (2d Cir. 1943) (holding that defendant unlawfully gave orders to make copies closely resembling copyrighted work without causing "copyright trouble").

[FN136]. Cross, 816 F.2d at 301.

[FN137]. That the copies were not sold for money was deemed irrelevant where hope of gain existed. Id. (citing Moore, 604 F.2d at 1235); see also United States v. Moran, 757 F. Supp. 1046, 1051 (D. Neb. 1991) (holding that defendant did not willfully violate copyright laws by creating copies of legally purchased video cassettes and renting those copies while retaining originals to guard against theft, based on testimony that he never simultaneously rented both copy and original).


[FN139]. Section 109(a) provides: "the owner of a particular copy ... lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy ...." 17 U.S.C. § 109(a) (1994).

[FN140]. Id. There must have been a lawful original sale of the work for the first sale doctrine to apply. See United States v. Larraecuent, 952 F.2d 672, 673 (2d Cir. 1992) (shifting burden to government to prove copies not legally made nor owned by defendant after defendant has met production burden of § 109 defense); United States v. Sachs, 801 F.2d 839, 842 (6th Cir. 1986) (requiring lawful sale to invoke first sale doctrine); United States v. Drum, 733 F.2d 1503, 1507 (8th Cir. 1984) (stating that government may prove absence of first sale either by evidence of source of the recordings, or by evidence that recordings were never authorized); American Int'l Pictures, Inc. v. Foreman, 576 F.2d 661, 663 (5th Cir. 1978) (requiring government to bear burden of negating first sale); United States v. Atherton, 561 F.2d 747, 749 (9th Cir. 1977) (reversing conviction due to government's failure to prove that copies sold by defendant had not been subject to first sale); Microsoft Corp. v. Harmony Computers & Elecs., 846 F. Supp. 208, 212 (E.D.N.Y. 1994) (holding that entering license agreement is not a "sale"). But see ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1453-55 (7th Cir. 1996) (holding "shrinkwrap" license, a package label limiting use of work, enforceable under state contract law, while not creating exclusive rights otherwise preempted by Copyright Act).

[FN142]. See L’anza Research Int’l v. Quality King Distrib., Inc., 98 F.3d 1109, 1117 (9th Cir. 1996) (holding that the first sale doctrine, under 17 U.S.C. § 109(a), does not bar defendant’s liability under 17 U.S.C. § 602(a) for re-importation of infringing goods lawfully sold abroad), cert. granted, 117 S. Ct. 2406 (1997), rev’d 118 S. Ct. 1125 (1998); see also BMG Music v. Perez, 952 F.2d 318, 319 (9th Cir. 1991) (stating that first sale doctrine does not provide defense to infringement by goods manufactured abroad). Interestingly, both L’anza and Sebastian involved hair-care products: the asserted copyright interest was in the bottle labels.

[FN143]. Quality King Distributors, Inc. v. L’anza Research Int’l, Inc., 118 S. Ct. 1125, 1134 (1998) (“[t]he whole point of the first sale doctrine is that once the copyright owner places a copyrighted item in the stream of commerce by selling it, he has exhausted his exclusive statutory right to control its distribution.”). However, the Supreme Court did not address “cases in which the allegedly infringing imports were manufactured abroad.” Id. at 1135 (Ginsburg, J., concurring). See generally Joan Biskupic, Court Lets Discounters Keep Selling U.S.-Made Goods They Buy Overseas, WASH. POST, Mar. 10, 1998, at A7 (noting concerns by U.S. manufacturers, including software and recording industries, that this decision would legitimize the multi-billion dollar “gray market” industry which undercut their domestic marketing).

[FN144]. See Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569  (1994) (finding that song which would otherwise infringe on copyright was fair use as parody); Leibovitz v. Paramount Pictures Corp., 948 F. Supp. 1214, 1219 (S.D.N.Y. 1996) (rejecting claim that all commercial use of protected elements of copyrighted work is de facto infringement).


[FN147]. See McDonald v. Multimedia Entertainment, Inc., 20 U.S.P.Q. 2d (BNA) 1372 (S.D.N.Y. 1991) (finding that single musical note or three-note sequence is too common to receive protection); Cain v. Universal Pictures Co., 47 F. Supp. 1013, 1017 (S.D. Cal. 1942) (describing small unprotected common details as "what the French call 'scènes à faire' "); see also Shipman v. RKO Radio Pictures, Inc., 100 F.2d 533, 536 (2d Cir. 1938) ("there is no infringement ... if the scene is considered by the court to be lacking in novelty so as to be regarded 'the common property of all playwrights' "); Sheldon v. Metro-Goldwyn Pictures Corp., 81 F.2d 49, 54-55 (2d Cir. 1936) (distinguishing themes and ideas as elements which may be copied under fair use from dramatic expression, which may not be copied under fair use). See generally WILLIAM PATRY, THE FAIR USE PRIVILEGE IN COPYRIGHT LAW 63-64, 465-66 (1985).

[FN148]. See PATRY, supra note 147, at 468-77.

[FN149]. See Sega Enterprises, Ltd. v. Accolade, Inc., 977 F.2d 1510, 1513 (9th Cir. 1993) (holding that reverse engineering undertaken for legitimate purpose is “as a matter of law a fair use of the copyrighted work”). But see Atari Games Corp. v. Nintendo of America, Inc., 975 F.2d 832, 843 (Fed. Cir. 1992) ("The fair use reproductions of a computer program must not exceed what is necessary to understand the unprotected elements of the work.").


[FN151]. Id. at 216. The defendants in Dowling taped, without authorization, commercially unreleased Elvis Presley performances and produced record albums. Id. at 214. The Supreme Court, citing the Copyright Act, concluded that
Congress had not intended for the National Stolen Property Act to apply to copyright infringement. Id. at 221-27.

[FN152]. See, e.g., United States v. Belmont, 715 F.2d 459, 461 (9th Cir. 1983) (applying Act to interstate transportation of "off the air" copies of motion pictures); United States v. Drebin, 557 F.2d 1316, 1328 (9th Cir. 1977) (holding that copies of copyrighted motion pictures constitute goods, wares or merchandise, and thus fall within the meaning of the Act).


[FN154]. See, e.g., United States v. Manzer, 69 F.3d 222, 229 (8th Cir. 1994) (using mail and telephone to sell unauthorized satellite decryption equipment); United States v. Shultz, 482 F.2d 1179, 1182 (6th Cir. 1973) (using mails to sell counterfeit sound recordings); Cooper v. United States, 639 F. Supp. 176, 180 (M.D. Fla. 1986) (using wires, specifically telephones, to distribute thousands of pirated sound recordings).


[FN156]. Id.


[FN158]. See generally, supra Part II.D of this Article (discussing RICO); cf. Schiller & Schmidt, Inc. v. Nordisco Corp., 969 F.2d 410, 414 (7th Cir. 1992) (dismissing RICO claim based on copyright infringement because plaintiff failed to prove substantial similarity); United States v. Drum, 733 F.2d 1503, 1506 (11th Cir. 1981) (applying RICO to charges arising out of sound recording copyright infringement business); United States v. Sam Goody, Inc., 506 F. Supp. 380 (E.D.N.Y. 1981) (holding that repeat copyright infringers who satisfied RICO criteria could not avoid prosecution on the ground they were not members of organized crime because RICO applies to any enterprise, both legal and illegal).


[FN163]. H.R. 2652, 105th Cong. § 1207(a).


concerns that such legislation would (1) overrule Feist Publications, Inc. v. Rural Telephone Serv. Co., 499 U.S. 340 (1991); (2) protect factual data beyond scope traditionally contemplated by Congress and Supreme Court; (3) provide renewable terms amounting to perpetual copyright; and (4) create government monopolies over information.


[FN167]. For a general overview of the elements of the criminal copyright offense, see supra Part IV.A.1 of this article.


[FN172]. The "Internet" refers to the on-line world and is used interchangeably with "cyberspace" and "Web." It is described as "an international network of interconnected computers" from which any number of users may access a "wide variety of communication and information retrieval methods." Reno v. American Civil Liberties Union, 117 S. Ct. 2329, 2334 (1997) (explaining and adopting Internet terminology).

[FN173]. 18 U.S.C. § 2319 (1994). Infringement of ten copies or phonorecords of one or more copyrighted works valued at more than $2,500 carries a maximum sentence of three years for a first offense and six for a second offense. Infringement of one or more copies or phonorecords which have a total retail value of more than $1,000 carries a maximum sentence of one year. 18 U.S.C. § 2319(b) (1994) amended by Pub. L. No. 105-47, § 2(d), 111 Stat. 2678, 2679 (1997).


[FN175]. The White House created the National Information Infrastructure Task Force ("IITF") in February 1992 to investigate regulatory needs for the on-line world. The IITF then formed the Working Group on Intellectual Property to examine the intellectual property implications of the National Information Infrastructure ("NII"). On July 7, 1994 the Working Group released a preliminary draft of its report, known as the "Green Paper." Following testimony and
public comments on this draft, the Working Group released in September 1995 a final version of the report, known as the "White Paper." Its main finding was that "with no more than minor clarification and limited amendment the Copyright Act will provide the necessary balance of protection of rights." WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 17 (1995) [hereinafter "WHITE PAPER"].


[FN177]. Downloading is the act of retrieving or accessing any information over the Internet. By way of contrast, "uploading" denotes placing files onto a server from which they may be accessed by anyone browsing the Web.

[FN178]. If the downloader is the equivalent of a record buyer, then just as the latter may legally turn around and resell her copy of the record, the former may resell whatever she downloaded. The difference between the two scenarios is that the record seller sacrifices her copy of the record, whereas the downloader likely retains a copy of what she downloaded. WHITE PAPER, supra note 175, at 95.

[FN179]. WHITE PAPER, supra note 175, at 95. Alternatively, copyright management systems can be used as a means for circumventing or monitoring subsequent use of downloaded programs. See Elizabeth Corcoran, Digital Information Protection Proposed; Device Would Stop Electronic Duplication, WASH. POST, Feb. 20, 1998, at G3 (noting concerns that such devices would not allow for fair use doctrine).


[FN183]. The entity that runs the on-line system or service.
[FN184]. See Sega Enter. Ltd. v. Maphia, No. CIV.A. 93-4262 CW, 1997 WL 337558, at * 1 (N.D. Cal. June 9, 1997) (permanently enjoining BBS operator from "displaying, transferring or making available" copyrighted videogames illegally copied by persons using BBS, upon finding owner knowingly facilitated infringement); Sega Enter. Ltd. v. Maphia, 857 F. Supp. 679, 683 (N.D. Cal. 1994) (holding defendant Sysop liable because it operated electronic bulletin board to which users uploaded plaintiff's copyrighted games, while other users downloaded them, and defendant had specific knowledge of, and at times even solicited, infringing actions); Playboy Enter. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993) (holding operator of computer BBS, which was accessible to customers for fee, liable for copyright infringement because users had downloaded plaintiff's unauthorized pictures); see also Playboy Enter. v. Russ Hardenburgh Inc., 982 F. Supp. 503, 511-12 (N.D. Ohio 1997) (collecting cases discussing direct or contributory infringement by BBS Sysop for allegedly displaying and distributing copyrighted documents placed on-line by subscribers). But see infra text accompanying notes 187-90 (offering reasons why Sysops should not be held liable for infringing activity occurring on their networks).


[FN186]. To hold a party liable for contributory infringement, the government must prove that the system provider willfully induced, caused, or substantially contributed to the infringing conduct. Casella v. Morris, 820 F. 2d 362, 365 (11th Cir. 1987); see also NIMMER & NIMMER, supra note 182, § 12.04(A)(2)(a).

[FN187]. See I. Trotter Hardy, The Proper Regime for "Cyberspace," 55 U. Pitt. L. Rev. 993 (1994) (analyzing whether on-line service providers ought to be exempt from liability or given a higher standard for liability if, for example, they are ignorant of, or unable to prevent, illegal behavior by users).


[FN189]. Id. at 1374 (holding that liability might exist where provider fails to remove infringing works after receiving notice of their posting on its network).

[FN190]. Id. at 1369. Legislation was introduced in February 1998 to codify Netcom and to overrule Playboy Enter. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993) (discussed supra note 184). On-Line Copyright Infringement Liability Limitation Act, H.R. 3209, 105th Cong. (1998); see also Introduction of the "On-Line Copyright Infringement Liability Limitation Act," 144 Cong. Rec. E160 (daily ed. Feb. 12, 1998) (statement of Rep. Coble, sponsor) (stating that this "bill essentially codifies the result in the leading and most thoughtful judicial decision to date [Netcom]. In doing so, it overrules those aspects of the Playboy v. Frena case, inasmuch as that case might apply to service providers")

[FN191]. WHITE PAPER, supra note 175, at 228-29. The requirement led the Working Group to conclude that current copyright law is "insufficient to prevent flagrant copyright violations in the NII context." Id. at 127-28.


[FN193]. Id. at 537.


[FN198]. Id. at 153 ("Warez crackers, traders, and collectors don't pirate software to make a living; they pirate software because they can. The more manufacturers harden a product with tricky serial numbers and anticopy systems, the more fun it becomes to break.").


[FN200]. Netcom, 907 F. Supp. at 1361; see also supra notes 187-90 and accompanying text.


[FN203]. Id. § 2(a), proposing new 17 U.S.C § 512(a).

[FN204]. Id. Authors of websites rent an amount of disk-space (fixed level of memory bytes) on the ISPs servers where they store hypertext mark-up language ("HTML," a website programming language) files, Javascript (a more advanced website programming language) files or other files, which are accessed by visitors to the site through their own web-browser and ISP. If the designer of the website pays a monthly fee for the telephone connection (dial-up) and an additional fee for the disk-space used to create the website, and the visitor to the site who downloads the illegal software pays a monthly fee for her dial-up, then both ISPs technically profited from the exchange of the illegal software. The bill seeks to eliminate such liability because neither ISP actively facilitated the exchange any more than a local telephone company actively facilitates a drug deal made over a cellular phone. Id.

[FN205]. See Legislation: House Subcommittee Holds Hearings on WIPO Treaty Bills, OSP Liability, BNA'S PAT., TRADEMARK & COPYRIGHT J., Sept. 18, 1997, at 413, 414 (describing concerns raised during hearing: that the act is either unnecessary since existing fair use and infringement protections are sufficient, or that the act may actually expose service providers to liability for providing "hyperlinks" (cross-references) to copyrighted materials).

[FN206]. Legislation, supra note 201, at 245.

[FN208]. Id.; see also Boyd v. Schildkraut Giftware Corp., 936 F.2d 76, 79 (2d Cir. 1991) (finding that impermissibly placing patent number on product by mistake does not constitute violation of false patent marking statute); cf. Arcadia Mach. & Tool v. Sturm, Roger & Co., 786 F.2d 1124, 1125 (Fed. Cir. 1986) (holding that label declaring contents of package "may be manufactured under" one or more of listed patents or pending applications did not violate false patent marking statute when box was used for various models).


[FN212]. Id.; see also Boyd, 936 F.2d at 79 (holding that cosmetic compact case manufacturer who misunderstood instructions to delete reference of patent holder’s patent number and shipped compacts with holder's number had not intended to deceive). But see Johnston v. Textron, Inc., 579 F. Supp. 783, 795-96 (D.R.I. 1984) (finding use of word "patented" in connection with radio advertising of unpatented article after being notified by patent holder of such false marking activity violated statute).


[FN217]. Id. at 227; see also United States v. LaMacchia, 871 F. Supp. 535, 537 (D. Mass. 1994) ("Dowling is a narrower case than [defendant] would have it, and holds only that copyright infringement does not satisfy the physical 'taking' requirement of the National Stolen Property Act").

[FN218]. See Dowling, 473 U.S. at 216 (finding that National Stolen Property Act "clearly contemplate[s] a physical identity between the items unlawfully obtained and those eventually transported" and finding language of copyright statutes to clearly distinguish possessory interests of copyright holder from ordinary property interests); see also Naso v. Park, 850 F. Supp. 264, 275 (S.D.N.Y. 1984) (holding that patent-infringing goods do not qualify under statute as stolen, converted or fraudulently-taken goods).

[FN219]. For the purpose of this section, the term "art crime" will be limited to fine arts such as paintings, sculptures and, to a lesser degree, antiquities and archaeological objects.
[FN220]. Ashton Hawkins, et al., A Tale of Two Innocents: Creating an Equitable Balance Between the Rights of Former Owners and Good Faith Purchasers of Stolen Art, 64 FORDHAM L. REV. 49, 49 (1995) ("[a]s the value of art transactions has now expanded, the theft of art and the trade in stolen art has kept pace"). Additionally, because the popularity of collecting art has driven up art prices, these elevated prices stimulate the criminal element in art theft. See JOHN E. CONKLIN, ART CRIME 21-33 (1994). Some estimates place art theft profits at $2 billion annually. See David Holmstrom, Stolen-Art Market Is a Big Business at $2 Billion A Year, CHRISTIAN SCIENCE MONITOR, Aug. 11, 1994, at 1; William Touhy, Picture This: Art Thievery is Thriving, L.A. TIMES, Aug. 16, 1994, at H1.

[FN221]. Touhy, supra note 220, at H1; cf. Anthony J. Del Piano, The Fine Art of Forgery, Theft and Fraud, CRIM. JUST., Summer 1993 at 16, 17 (contending that art theft is second only to illicit drug market).

[FN222]. Theft and vandalism of art, despite their often tremendously costly and devastating effects, usually do not demand the degree of sophistication that characterizes white collar crime, and therefore this section will not deal with such offenses; however, the subsequent resale or laundering of stolen art is a major element of white collar art crime. See Del Piano, supra note 221, at 18 (noting that trafficking of stolen art transforms simple thefts into complex criminal enterprises). For review and discussion on the use of civil actions to seek relief in art crimes, see Steven A. Bibas, Note, The Case Against Statutes of Limitations for Stolen Art, 103 YALE L.J. 2437 (1994), in which the author rejects property approaches to art crimes and argues for the elimination of statute of limitation bars for victims who report art thefts. See also Hawkins, et al., supra note 220 (advocating legislative balancing of rights and duties among former owners, sellers and purchasers); William G. Pearlstein, Claims for the Repatriation of Cultural Property: Prospects for a Managed Antiquities Market, 28 LAW & POLY INT'L BUS. 123 (1996) (analyzing patrimony claims and proposing managed antiquities market).


[FN224]. For example, the Drug Enforcement Agency (DEA) staged "Operation Dinero" to uncover money laundering by the Cali Columbia drug cartel; this netted three paintings attributed to Picasso, Rubens and Reynolds. See Anna J. Kisluk, DEA Operation Nets 3 Pictures, IFAR REP., Dec. 1995, at 6, 8 (reporting that Operation Dinero proved that "drug money was being laundered by the buying and selling of works of art"); see also Customs Auction of a Dali Accents Laundering by Art, MONEY LAUNDERING ALERT, June 1, 1995 (noting the "large disparity between cash bank deposits made by auction houses and cash receipts reported by them on IRS Form 8300"); Jo Durden-Smith, Masterpieces as Money, TOWN & COUNTRY MONTHLY, July 1, 1996, at 30 (concluding that art works are just another form of money). For a general discussion of money laundering, see the MONEY LAUNDERING article in this issue.

[FN225]. Possible frauds include fraudulent appraisals and authentication, insurance fraud, tax fraud, investment fraud, fraud by corporate collectors, fraudulent bidding practices, consignment fraud, customs violations, selling stolen and counterfeit art, buying stolen art, inflation of attendance figures, and passing bad checks. See CONKLIN, supra note 220, at 87-117 (discussing many fraudulent activities in the art world).

[FN226]. See generally HECTOR FELICIANO, THE LOST MUSEUM: THE NAZI CONSPIRACY TO STEAL THE WORLD'S GREATEST WORKS OF ART (1997) (tracing artwork confiscated by the Third Reich during World War II); LYNN H. NICHOLAS, THE RAPE OF EUROPA: THE FATE OF EUROPE'S TREASURES IN THE THIRD REICH AND THE SECOND WORLD WAR (1994) (discussing thefts during the war by German and Soviet troops and immediately after the war by American troops who were guarding the Nazi art stockpiles). The "Quedlinburg Treasures," worth an estimated $200 million, were stolen from Germany by an American soldier;
upon his death, when his brother and sister sold some works and attempted to sell others, they were charged under the National Stolen Property Act. WILLIAM H. HONAN, TREASURE HUNT: A NEW YORK TIMES REPORTER TRACKS THE QUEDLINBURG HOARD 275-82 (1997); see also NICHOLAS, supra, at 355-56, 442-43 (discussing Quedlinburg Treasures); William H. Honan, 3 Are Indicted in Sale of German Art Stolen by G.I., N.Y. TIMES, Jan. 5, 1996, at A10 (noting that defendants "could be imprisoned up to five years and fined up to $250,000," as well as face $30 million in inheritance taxes); Peter Watson, Looted!, DAILY TELEGRAPH (London), July 20, 1996, at 21 (same). But see Lee Hancock, W.W.II Art Theft Case Is Thrown Out of Court, WASH. POST, Oct. 24, 1996, at D7 (stating that judge ordered charges dismissed since indictment was obtained "one day too late under the federal statute of limitations;" however, IRS claim remains active); William H. Honan, U.S. Revives Art Theft Case, N.Y. TIMES, Jan. 24, 1997, at C1 (noting subsequent appeal). Both parties appealed the trial court's decision to the Fifth Circuit, Docket Nos. 97-40022 (U.S. appeal) and 97-40144 (defendant's appeal), and oral arguments were heard on Jan. 6, 1998.

The general issue of restitution of art works stolen during World War II has cast a significant cloud over both the art market and the holdings of some art museums, since the victims may be able to recover the art works from collectors or museums who have held them for several decades. See, e.g., Alexandria Peers, Austria to Auction "Spoils-of-War" Art, to Benefit Victims, WALL ST. J., May 29, 1996, at A4 (observing that victims' "claims have become a 'hot-button' issue in the art world"). One recent episode was an attempt by the U.S. District Attorney for Manhattan to block the return to Austria of two works, loaned to the Museum of Modern Art (N.Y.) for an exhibit on the Austrian painter Egon Schiele, on the grounds that these works were illegally confiscated in 1940 and should be returned to the descendants of the pre-war owner, and not the current Austrian owner. See Judith H. Dobrzynski, More Paintings by Schiele Face Ownership Questions, N.Y. TIMES, Jan. 15, 1998, at B4 (noting that an additional sixteen Schiele works now in the United States face similar ownership challenges); see also Judith H. Dobrzynski, Man in the Middle of the Schiele Case, N.Y. TIMES, Jan. 9, 1998, at E2 (describing activities of World Jewish Congress's Commission for Art Recovery, which is receiving daily average of one inquiry about disputed or missing works). This problem was the subject of congressional hearings in February 1998. Holocaust Victims' Claims: Hearings Before the House Banking & Fin. Serv. Comm., 105th Cong. (Feb. 12, 1998); see also Jacqueline Trescott, The Art Plunder Problem; Panel Told of Efforts to Deal With Nazi Loot, WASH. POST, Feb. 13, 1998, at D2 (noting that while such cases are few, "they have shaken the art world").


[FN228]. See CONKLIN, supra note 220, at 61 (estimating "that Dalí signed 350,000 blank sheets of art paper in his career," used to make inexpensive photographic reproductions, which were marketed as high-priced "originals" or "limited editions").


[FN230]. See Steven Mark Levy, Liability of the Art Expert for Professional Malpractice, 1991 WIS. L. REV. 595, 596 ("fine arts experts, including authenticators, appraisers and consultants, wield tremendous financial power in the art market").

[FN231]. See, e.g., Denise M. Topolnicki & J. Howard Green, The Fine Art of Fraud, MONEY, Sept. 1986, at 73 (asserting that collectors may often be reticent to report fraud, for example due to embarrassment, desire to not call
attention to their art collection for fear of robbery or IRS audit, to continue deception in order to sell the piece, or because they are reluctant to question the legitimacy of other pieces in their collection). Furthermore, there is no simple either-or dichotomy between authentic and fake art works. See R.H. MARINISSEN, PAINTINGS, GENUINE, FRAUD, FAKE: MODERN METHODS OF EXAMINING PAINTINGS 20-34 (1985) (listing fifteen categories of "authenticity").

The Art Loss Register ("ALR") maintains an international, permanent, computerized clearinghouse on stolen and missing art; their image database of over 60,000 items has been instrumental to the recovery of numerous stolen objects. For more information regarding ALR, see the Art Loss Register's Website: <http://www.artloss.com/>. The International Foundation for Art Research ("IFAR"), a non-profit organization dedicated to preventing and recovering stolen, forged and misattributed art works, maintains the ALR's U.S. office and can be reached at 500 Fifth Avenue, Suite 1234, New York, NY 10110 (tel. 212-391-6234; fax 212-391-8794; email alrnewyork@aol.com). See generally Barbara Lantin, The Art of Helping Police with Inquiries, INDEPENDENT (London), Apr. 3, 1996 (discussing role of the Art Loss Register).

The Getty Information Institute, Los Angeles, has established the "Getty Provenance Index" which documents the provenance (history of ownership) of over a half-million art works, which are coded by means of their "Object ID Checklist." This database is currently on a CD-ROM and will eventually be posted on the Internet. See Getty Information Institute, The Work of the Getty Provenance Institute (visited Feb. 19, 1998) <http://www.gii.getty.edu/provenance/index.html> (describing these databases).

The complexity and expense of accurate authentication also impedes detection. See Lawrence S. Bauman, Note, Legal Control of the Fabrication and Marketing of Fake Paintings, 24 STAN. L. REV. 930, at 935-36 (1972) (pointing out the unavailability of art experts for the purposes of authentications and providing several reasons for this problem). For examples of high-priced scientific authentication techniques, see David Conrads, Progress Is Real for Those in the Business of Spotting Fakes: Scientists and Art Historians Are Erecting a Formidable Barrier Between Art Forgers and Art Museums, CHRISTIAN SCIENCE MONITOR, Oct. 8, 1996, at 12; Leonard D. Du Boff, Controlling the Artful Con: Authentication and Regulation, 27 HASTINGS L.J. 973, 988-97 (1976).

A San Francisco high-technology firm has developed a digital registration process, "ISIS," (Intrinsic Signature Identification System) that could help resolve disputes about authenticity and ownership of art works, thereby discouraging forgery and theft. The process is "based on the premise that all objects contain unique microscopic physical features and random anomalies that cannot be duplicated." Suzanne Muchnic, Have Forgers Finally Met Their Match?: A New Digital Registration Process Could Discourage Forgery and Theft and Help Resolve Disputes About Authenticity and Ownership of Valuable Artworks, L.A. TIMES, Jul. 2, 1995, at Calendar 50 (concluding that success of this project remains uncertain). For further information on ISIS, see Verification Technologies, Inc., Main Page (last modified Apr. 16, 1997) <http://www.netventure.com/vti/isis>.

[FN232]. The vulnerability of novice collectors and their willingness to rely on a dealer's reputation instead of researching their purchases often facilitates the commission of art crime, despite the typically unskilled nature of the perpetrators. See Robin Morris Collin, The Law and Stolen Art, Artifacts, and Antiquities, 36 HOW. L.J. 17, 27 (1993) (stating that consumers seldom inquire into legitimacy of art work); Topolnicki & Green, supra note 231, at 73 (pointing out that victims of many art frauds are usually novice collectors); cf. Balog v. Center Art Gallery-Hawaii, Inc., 745 F. Supp. 1556, 1562 (D. Haw. 1990) ("some well-executed fakes have fooled even knowledgeable buyers and dealers"); Bauman, supra note 231, at 932-34 (citing numerous methods of forgery, such as faked signatures, completions of unfinished canvases, misrepresentation of a work's author, reproductions, pastiches [a method of combining elements of several works to create a new work], and faked unfinished drawings).

[FN233]. See Bauman, supra note 231, at 931 (asserting that existing state and federal regulatory attempts to control art crime frequently fail since available statutes for prosecution of art crime are primarily intended for other purposes, thus requiring creative tailoring to be of much use); Du Boff, supra note 231, at 998 (stating that such statutes may also be ineffective because their penalties are insufficient deterrents in light of the potential profits). Faced with this statutory futility, prosecutors frequently choose not to waste precious funds and time on a losing battle. See also Balog, 745 F. Supp. at 1564 (stating that a dealer's authentication of a work, unless that dealer witnessed work being produced, "can never be more than an educated guess or opinion"); Du Boff, supra note 231, at 998 (asserting that intent requirement for fraudulent authentication may encourage sellers to intentionally not authenticate works).
The theft of major artwork statute was part of a much larger omnibus bill, and there appears to be no legislative history specifically addressing this statute.

"Museum" is broadly defined to cover organized and permanent institutions that (a) are in the United States; (b) are "established for an essentially educational or aesthetic purpose;" (c) have a professional staff; and (d) own and regularly display to the public tangible objects.

"Object of cultural heritage" is defined to encompass any object that is either (a) over 100 years old and worth over $5,000, or (b) worth at least $100,000, regardless of age.

For a general discussion of mail and wire fraud, see the MAIL AND WIRE FRAUD article in this issue.

Additionally, the defendants were charged with securities fraud. For a general discussion of securities fraud, see the SECURITIES FRAUD article in this issue.

The gallery's president was fined $750,000 and given a three year prison sentence, and the vice-president was fined $282,000 and given a two-and-a-half year prison sentence. They were also ordered to pay restitution.

In addition to the criminal prosecution, see supra note 240, there was parallel civil litigation based upon the same conduct.


[FN247]. See CATTERALL, supra note 223, at 96.

[FN248]. In United States v. Amiel, 813 F. Supp. 958 (E.D.N.Y.), aff'd, 995 F.2d 367 (2d Cir. 1993), involving the prosecution of forgers and the dealers of the forgeries, the government prosecuted four members of the Amiel family for mail fraud and conspiracy. The defendants were running what was reputed to be "the single largest worldwide source and distribution network of bogus prints." Also prosecuted was at least one dealer of the Amiel's works who pled guilty to mail fraud. David S. Hilzenrath, Cracking Down on Counterfeit Art; U.S. Charges 4 in the Global Distribution of Bogus Prints, WASH. POST, Jan. 31, 1992, at C1.


[FN250]. See Bauman, supra note 231, at 939 (noting limited use of copyright laws in art crimes prosecution).

[FN251]. Id.


[FN256]. See generally Carl Nagin, Hot Art: Illegal Traffic in Antiquities, TOWN & COUNTRY MONTHLY, Mar. 1, 1995, at 138 (discussing the effectiveness of this committee despite its "cumbersome bureaucratic process").

[FN257]. Final Act of the Diplomatic Conference for the Adoption of the Draft UNIDROIT Convention on the
International Return of Stolen or Illegally Exported Cultural Objects, June 24, 1995, 34 I.L.M. 1322. The final title of the treaty is "UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects."

[FN258]. Id. at 1334-35, Article 10 (stating that provisions shall apply prospectively, not retroactively).

[FN259]. See List of the States Which Signed the Convention (visited Jan. 23, 1998) <http://www.tufts.edu/departments/fletcher/multi/www/unidroit95-rat.html> (listing 22 signatories). As of January 1998, Lithuania, Paraguay, and Romania have ratified the UNIDROIT treaty while China and Ecuador have acceded to it. On January 21, 1988 the fifth ratification instrument was deposited by Romania with the Italian government. Consequently, pursuant to Article 12, paragraph 1 (UNIDROIT, Ch. 5, Art. 12(1), 34 I.L.M. at 1335), the treaty will enter into force between these five nations on July 1, 1998. Letter from Marina Schneider, Research Officer, Unidroit Secretariat (Feb. 12, 1998) (on file with the American Criminal Law Review) (noting "that Peru and Hungary have already passed the law permitting the ratification and we are waiting for the formal deposit of the instruments"); see also Richard P. Greenfield, The Trouble with the Trojan Gold, NEWSDAY (N.Y.), Jan. 7, 1996, at A38 (explaining why United States has abstained from voting on UNIDROIT convention); Kimbell to Host Swiss Collection: Paintings Find Temporary Sanctuary in Fort Worth, DALLAS MORNING NEWS, Jul. 5, 1997, at 43A (discussing problems in the ratification process). For general discussion and analysis of UNIDROIT, see Marina Schneider, The UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects (visited Sept. 14, 1997) <http://www.city.ac.uk/artspol/schneider.html>; see also Jennifer Howard, Objects of Desire; Contested Artifacts Are the Prize in an International Culture Clash, WASH. POST, Dec. 14, 1997, at C1, C5 (describing inherent complications in repatriating artistic and cultural objects); Brian Bengs, Note, Dead on Arrival? A Comparison of the UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects and U.S. Property Law, 6 TRANSNAT'L L. & CONTEMP. PROBS. 503 (1996) (analyzing potential effects of UNIDROIT on United States property law).

[FN260]. See, e.g., Godfrey Barker & Laura Stewart, The Arts: Maastricht-- the Last Art Fair?, DAILY TELEGRAPH (London), Mar. 11, 1996, at 18 (claiming that if The Netherlands ratifies this treaty, art dealers will move their annual fair from Maastricht to a non-ratifying country); Hawkins, et al., supra note 220, at 86 ("[i]f adopted, UNIDROIT would effectively supplant the CPIA").

[FN261]. See, e.g., N.Y. ARTS & CULT. AFF. § 3.01 (McKinney 1984) (stating promotion of the arts as statutory goal).

[FN262]. Section 170.45 of the New York Penal code states:

A person is guilty of criminal simulation when:

1. With intent to defraud, he makes or alters any object in such manner that it appears to have an antiquity, rarity, source or authorship which it does not in fact possess; or

2. With knowledge of its true character and with intent to defraud, he utters or possesses an object so simulated. Criminal simulation is a class A misdemeanor.


[FN263]. Former N.Y. PENAL § 959 was aimed at "[t]he reproduction or forgery of archeological objects." Staff Notes of the Commission on Revision of the Penal Law, N.Y. Penal § 170.45.

[FN264]. Id.; see also N.Y. ARTS & CULT. AFF. § 13.03 (McKinney Supp. 1997) (falsifying certificates of authenticity for a work of fine arts is a class A misdemeanor).

These three states are Florida, Montana, and South Dakota. See Fla Stat. ch. 267.13 (1993) (limiting application to "any archaeological or historical object"); Mont. Code Ann. § 22-3-441 (1995) (limiting application to "heritage property or paleontological remains;") the former refers to Native American objects; S.D. Codified Laws Ann. § 1-20-37 (Michie 1992) (limiting application to "any archaeological, paleontological, ethnological or historical" objects).

See Cal. Civil Code § 1744(a)(10), 1745 to 1745.5 (West 1985 & Supp. 1997) (requiring disclosure of the total size of limited editions with a penalty not to exceed $1,000 for each violation); 815 Ill. Comp. Stat. § 345/0.01-9 (West 1997) (same).

In February 1987, the New York Attorney General’s Office obtained the first felony convictions in the nation against the operators of a telephone boiler-room gallery in its conspiracy prosecution of four defendants in the Carol Convertine Gallery case. Topolnicki & Green, supra note 231, at 73. The defendants reached potential customers over the telephone and by mailing brochures and price lists and providing false certificates of authentication. Two defendants pleaded guilty to conspiracy, and two others were convicted of nine counts of fraud. One defendant was convicted of an additional eight misdemeanor counts for the issuance of the false certificates. CONKLIN, supra note 220, at 82-83. The gallery was in part supplied by another member of the Amiel family, Douglas C. McGill, Fake Art Prints: Big Business Getting Bigger, N.Y. TIMES, July 22, 1987, at A1; see also United States v. Amiel, 813 F. Supp. 958, 959 (E.D.N.Y. 1993) (describing the convictions obtained in that prosecution). In related civil litigation, a French corporation which claimed an exclusive license in Dalí’s works filed a civil RICO suit, under 18 U.S.C. § 1962(c) (enterprise involvement in racketeering), based on predicate acts of money laundering, mail fraud and wire fraud. See Galerie Furstenberg v. Coffaro, 697 F. Supp. 1282 (S.D.N.Y. 1988) (dismissing plaintiff’s money laundering, conspiracy, and trademark claims, but allowing civil RICO suit based solely on mail and wire fraud acts).

See People v. Mahboubian, 543 N.E.2d 34, 36 (N.Y. 1989) (discussing defendants’ attempts to defraud insurance company by staging theft of art forgeries and collecting on the value of authentic pieces); cf. Bill Callahan, Art Dealer Sentenced in Wieghorst Swindle, SAN DIEGO UNION-TRIB., Sept. 27, 1989, at B3 (citing an unreported California case in which art dealer Louis Almeida was convicted on six counts of grand theft, carrying a sentence of up to seven and one half years in state prison, for selling forgeries of the paintings of Olaf Wieghorst).


convictions).


[FN273], 18 U.S.C.A. § 1832(a)(5) (Supp. 1998). Section 2B1.1 also applies to thefts of trade secrets violations as defined under § 1832. See discussion supra note 272 (addressing amendment to § 2B1.1).


[FN277], Id. Section 2314 was amended in 1994 to remove the outdated maximum fine. Pub. L. No. 103-322, Title XXXIII, § 330016(1)(L), 108 Stat. 1796, 2147 (1994).

[FN278], U.S.S.G. App. A (1998). For an application of this Act to a particular type of intellectual property crime, refer to the sentencing provisions of the applicable section of this article.


[FN282], U.S.S.G. § 2B1.1(b)(4)(B) (1998); see also United States v. Collins, 104 F.3d 143, 144 (8th Cir. 1997) (upholding sentence increase of four levels for being in business of receiving and selling stolen goods, as defined by 18 U.S.C. § 2314).

[FN283], 18 U.S.C. § 1905 (1994). This Act only applies to public officers and public employees. Id.

[FN284], Id. The Act makes it a misdemeanor for any employee of the United States to disclose trade secrets "[t]o any extent not authorized by law." Id.


[FN293]. U.S.S.G. § 2F1.1(b)(1) (1998); see also United States v. Austin, 54 F.3d 394, 402 (7th Cir. 1995) (upholding sentence based on sales revenue of $3.8 million, even though the art works "were worthless fakes" having no value).

[FN294]. U.S.S.G. § 2F1.1(b)(2) (1998); see United States v. Austin, 103 F.3d 606, 608 (7th Cir. 1997) (upholding upward adjustment in sentencing for more than minimal planning and for organizing or supervising more than five persons); United States v. Mett, 65 F.3d 1531, 1537 (9th Cir. 1995) (same); United States v. Ellerbee, 73 F.3d 105, 108 (6th Cir. 1996) (upholding two-level enhancement of sentence based on evidence of "more than minimal planning," which could be deduced by "more planning than is typical, repeated acts, and steps to conceal the crime").


[FN301]. 18 U.S.C. § 2320(b) (1994); see also Vuitton v. White, 945 F.2d 569, 575-76 (3d Cir. 1991) (discussing requirements for relief under the ex parte seizure provision of the Act).


[FN303]. 18 U.S.C. § 2319(b)(1) (1994). The Copyright Felony Act does not require that all affected copyrights be of the same class or held by the same copyright owner. Saunders, supra note 107, at 690. The ten copies or phonorecords can be an aggregation of works by different authors, allowing for the establishment of a case of criminal copyright infringement against an infringer who has adversely affected several different copyright holders. Id. As stated in United States v. Larracuente, 952 F.2d 672 (2d Cir. 1992), the definition of "retail value" in cases involving copies of good quality is "the suggested retail price of the legitimate copyrighted work when it was released and not the value of the infringing copies." See also Roger J. Miner, Considering Copyright Crimes, 42 J. COPYRIGHT SOC'Y U.S.A. 303, 310 (1995).

[FN304]. Saunders, supra note 107, at 690.


[FN307]. 18 U.S.C. § 3571(d) (1994) reads as follows: Alternative fine based on gain or loss.--If any person derives pecuniary gain from the offense, or if the offense results in pecuniary loss to a person other than the defendant, the defendant may be fined not more than the greater of twice the gross gain or twice the gross loss, unless imposition of a fine under this subsection would unduly complicate or prolong the sentencing process. 18 U.S.C. § 3571(d) (1994). For an example of the application of the Sentencing Guidelines to copyright felonies, see Larracuente, 952 F.2d at 674-75.


[FN319]. "An instruction to use a particular subsection or table from another offense guideline refers only to the particular subsection or table referenced, and not to the entire offense guideline," U.S.S.G. § 1B1.5(b)(2) (1998). But cf. Miner, supra note 303, at 307 (criticizing the U.S.S.G. penalties for copyright felonies as "much too low").


[FN324]. 18 U.S.C. § 3571(b) (1994) (outlining fines for individuals); 18 U.S.C. § 3571(c) (1994) (setting forth fines for organizations); 18 U.S.C. § 3571(d) (1994) (stating that fine equals twice gross gain or loss when violators have pecuniary gain or if the victim suffer loss).


END OF DOCUMENT