APPENDIX A – EXECUTIVE ORDER 13,133

WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to address unlawful conduct that involves the use of the Internet, it is hereby ordered as follows:

Section 1. Establishment and Purpose.

(a) There is hereby established a working group to address unlawful conduct that involves the use of the Internet ("Working Group"). The purpose of the Working Group shall be to prepare a report and recommendations concerning:

(1) The extent to which existing Federal laws provide a sufficient basis for effective investigation and prosecution of unlawful conduct that involves the use of the Internet, such as the illegal sales of guns, explosives, controlled substances, and prescription drugs, as well as fraud and child pornography;

(2) The extent to which new technology tools, capabilities, or legal authorities may be required for effective investigation and prosecution of unlawful conduct that involves the use of the Internet; and

(3) The potential for new or existing tools and capabilities to educate and empower parents, teachers, and others to prevent or to minimize the risks from unlawful conduct that involves the use of the Internet.

(b) The Working Group shall undertake this review in the context of current Administration Internet policy, which includes support for industry self-regulation where possible, technology-neutral laws and regulations, and an appreciation of the Internet as an important medium both domestically and internationally for commerce and free speech.

Section 2. Schedule. The Working Group shall complete its work to the greatest extent possible and present its report and recommendations to the President and Vice President within 120 days of the date of this order. Prior to such presentation, the report and recommendations shall be circulated through the Office of Management and Budget for review and comment by all appropriate Federal agencies.

Section 3. Membership.

(a) The Working Group shall be composed of the following members:

(1) The Attorney General (who shall serve as Chair of the Working Group);

(2) The Director of the Office of Management and Budget;

(3) The Secretary of the Treasury;

(4) The Secretary of Commerce;

(5) The Secretary of Education;

(6) The Director of the Federal Bureau of Investigation;

(7) The Director of the Bureau of Alcohol, Tobacco and Firearms;

(8) The Administrator of the Drug Enforcement Administration;

(9) The Chair of the Federal Trade Commission;[1]

(10) The Commissioner of the Food and Drug Administration; and

(11) Other Federal officials deemed appropriate by the Chair of the Working Group.

(b) The co-chairs of the Interagency Working Group on Electronic Commerce shall serve as liaison to and attend meetings of the Working Group. Members of the Working Group may serve on the Working Group through designees.

WILLIAM J. CLINTON

THE WHITE HOUSE,
August 5, 1999

[1] Although the Chair of the Federal Trade Commission ("FTC") served as a member of the Working Group, the FTC has not, as an independent federal agency, taken a position on the views expressed in this report.

APPENDIX B – INTERNET FRAUD

1. Nature of the Potentially Unlawful Conduct

The electronic marketplace offers consumers unprecedented choice and convenience, and it gives businesses of all kinds low-cost access to a global consumer base. With these benefits, however, comes the challenge of ensuring that the virtual marketplace is a safe and secure place to purchase goods, services, and digitized information.

As commerce on the Internet grows, law enforcement agencies are observing a growing variety of fraudulent schemes that use the Internet, either to communicate false or fraudulent representations to prospective victims or to obtain valuable information or resources necessary for the success of the schemes. In 1998, for example, roughly 8,000 Internet-related complaints were entered into Consumer Sentinel, a consumer fraud database administered by the Federal Trade Commission ("FTC") and used by over 220 law enforcement agencies across the United States and Canada. In 1999, Consumer Sentinel received over 18,600 Internet-related complaints, more than double the prior year's number.[1]

One form of Internet fraud that is of particular concern is that of "identity theft," which generally involves obtaining data from individual consumers' financial transactions on the Internet or elsewhere, and either billing the consumers' credit cards for nonexistent transactions or services or using consumers' personal data to conduct actual transactions that are billed to the consumers. Other Internet fraud schemes include so-called "pyramid schemes";[2] entities that purport to be Internet banks that offer above-market rates for deposits; companies that promise to repair consumers' credit, but that do nothing after taking consumers' money; companies that purport to offer investments in nonexistent items, such as "prime bank" securities or software to solve the Y2K problem; companies that are thinly traded on securities markets or in fact are merely shell companies; and companies that fraudulently offer to sell Internet-related goods and services, or collectible goods through online auctions. Finally, some fraud schemes combine use of Internet websites with telemarketing "boiler rooms" to enhance direct contact with prospective victims.

---

[1] Consumer Sentinel aggregates data received by the FTC and by partners such as Internet Fraud Watch, a project of the non-profit National Consumers League, and over 50 major Better Business Bureaus. To develop additional information about the scope and volume on Internet fraud, several agencies are also supporting the establishment of an Internet Fraud Complaint Center, a joint project of the FBI and the National White Collar Crime Center, and are exploring the development of studies that could produce reliable estimates of Internet fraud.

[2] A "pyramid scheme" is generally a scheme in which the operators of the scheme try to obtain funds from several successive groups of investors and then use funds obtained from more recent investors to pay a portion of the funds owed to earlier investors, while retaining substantial proceeds from the scheme.

2. Analysis of Existing Law

Each of the Internet fraud schemes described above may violate one or more of the general federal criminal statutes dealing with fraud – such as credit card fraud, *see* 15 U.S.C. § 1644, 18 U.S.C. § 1029; financial institution fraud, *see* 18 U.S.C. § 1344; mail fraud, *see id.* § 1341; and wire fraud, *see id.* § 1343 – as well as specialized federal criminal statutes that prohibit money laundering, *see id.* § 1956, and identity theft, *see id.* § 1028. The FBI has jurisdiction to investigate violations of each of these statutes, and the Postal Inspection Service has jurisdiction to investigate most of these violations as they relate to mail fraud schemes. In addition, the Secret Service has jurisdiction to investigate credit card fraud and identity theft, and the Internal Revenue Service has jurisdiction to investigate money laundering. The Customs Service and Secret Service also have jurisdiction over some of the predicate offenses related to money laundering. (As discussed in Appendix H below, the Securities and Exchange Commission has jurisdiction to investigate violations of the federal securities laws.) And, the Department of Justice, through its Criminal and Civil Divisions and local U.S. Attorneys' Offices, conducts criminal prosecutions of these fraud schemes and may seek civil injunctive relief under 18 U.S.C. § 1345.

> ***"We must give consumers the same protection in our virtual mall they now get at the shopping mall."***
>
> **President Bill Clinton**
> **November 1998**

In addition, the FTC has authority to bring civil actions against fraudulent Internet schemes under the FTC Act, which prohibits unfair and deceptive acts or practices, 15 U.S.C. § 45(a). The FTC is also authorized to seek injunctions and other equitable relief in federal court, *id.* § 53(b), and may obtain a temporary restraining order that freezes a defendant's assets and results in the appointment of a temporary receiver.

Because these federal criminal and civil laws make no distinction between fraudulent representations over a telephone or fax machine and fraudulent representations posted on an online bulletin board or website, federal substantive law appears generally adequate to address Internet fraud. Since 1995, for example, the FTC has brought over 100 Internet-related cases, obtained permanent injunctions against dozens of Internet-related schemes, collected over $20 million in redress for victims of online fraud, and frozen another $65 million in cases currently in litigation. An Illinois man was recently sentenced to six months home confinement and probation for three years for conducting a million dollar mail-fraud scheme that involved the use of a website to solicit investors in oil and gas drilling ventures. And five individuals were recently convicted in an online scam in which the perpetrators stole the identities of legitimate vendors and advertised and sold non-existent products to their victims, resulting in losses to the victims of over $50,000.

3. Specific Federal Initiatives

The FTC has undertaken an array of initiatives to combat online fraud, including:

Project SafeBid – Online auction fraud is the most common Internet-related problem reported by consumers. Thousands of individuals have been

"winning bidders" on an Internet auction, sent money to the seller, but never received their goods. To address this problem, the FTC initiated Project SafeBid, disseminating educational materials to consumers, encouraging fraud prevention by Internet auction sites, and providing training and support to law enforcement agencies around the country in their efforts to stop Internet auction fraud artists. Project SafeBid has also generated over 40 case referrals, resulting in eight criminal or civil actions to date.

Operation Cure.All – In 1997 and 1998, the FTC led two "surf days" to target "miracle cures" for serious illnesses. After these surfs, the FTC and the FDA brought several cases against marketers of products such as magnetic therapy devices and shark cartilage for claims that these products could cure cancer, HIV/AIDS, multiple sclerosis, arthritis, or other diseases.

Website "Cramming" Sweep – The FTC has brought five federal court cases against 20 defendants, alleging that they placed unauthorized charges on small business' telephone bills for website services that the defendants promoted as "free." The defendants collectively solicited over one million small businesses nationwide. The FTC's Small Business Alliance for Fraud Education ("SAFE") also helped disseminate fraud warnings to the business community.

FTC's Internet Lab – In September 1999, the FTC unveiled a new Internet Lab with high-technology tools to investigate high-technology consumer problems. The lab allows investigators to search for fraud and deception on the Internet in a secure environment and provides staff with the necessary

Page-Jacking – A New Type of Computer Crime?

Page-jacking involves the appropriation of website descriptions, key words, or meta-tags from other sites. The page-jacker inserts these items into his own site, seeking to draw consumers to a particular site. This is because the descriptions, key words, and meta-tags are used by search engines when sorting and displaying sites on a particular topic requested by an individual. When the sites for a particular topic appear, an individual might see two or three descriptions for what appear to be the same site. If a person happens to click on one of the duplicated descriptions, he or she will be directed to the "fake site," which often is a pornographic site. Complicating matters even further is that page-jackers often "mouse-trap" a user's browser so that attempts to close the browser's windows or to use the "back" or "forward" button will simply direct the user to another pornographic site.

The FTC has taken the lead in addressing page-jacking. In September 1999, the FTC announced that it had obtained temporary restraining orders in federal district court against several website owners for page-jacking. The FTC alleged that the website owners engaged in deceptive and unfair trade practices in violation of the FTC Act, 15 U.S.C. § 45(a). Page-jacking could also potentially violate federal intellectual property laws. That is, if a page-jacker copies substantial portions of the imitated sites, then he might be criminally liable for copyright infringement. In addition, if a page-jacker hacks into a domain name server and changes the data to redirect visitors to the hacker's site, that person could also be in violation of federal computer crime statutes, such as 18 U.S.C. § 1030, which protect the integrity of computer systems against hackers.

equipment to preserve evidence for presentation in court. The lab also provides a means to train FTC staff and other law enforcement agents on new investigative techniques. The FTC's Internet Lab was instrumental in a recent "page-jacking" case (see sidebar above) that halted a global scheme in which millions of webpages were manipulated and unsuspecting consumers were driven to unwanted adult websites.

The Department of Justice, in coordination with the FTC, the FBI, and other agencies, is also actively pursuing online fraud as part of its Internet Fraud Initiative, announced by the Attorney General in February 1999. These efforts include prosecuting Internet-related fraud schemes such as securities and investment schemes, online auction schemes, and bank fraud; training prosecutors and agents on online fraud; developing online investigative and analytical resources; providing interagency coordination on online fraud prosecutions; and conducting public education and prevention efforts (*e.g.*, a website on identity theft and fraud (www.usdoj.gov/criminal/fraud/idtheft)).

In addition, because most Internet fraud schemes (and, for that matter, non-Internet fraud schemes) rely on the use by victims of the U.S. mails or private courier to make payments, the Postal Inspection Service is working with international postal administrators – most notably in Canada, Nigeria, and Ghana – to identify and to intercept victims' payments that are destined for addresses identified with fraud promotions. In addition to such cooperative administrative efforts, law enforcement agencies can combat fraud through the use of civil injunctive powers, such as temporary restraining orders on mail, false representation orders, and injunctions against fraud.

The Consumer Product Safety Commission ("CPSC") has stepped up its role in an area that complements the battle against online fraud: the need to ensure that products sold over the Internet (like other products sold) are safe. Products sold online must meet the same safety standards as products sold in brick-and-mortar stores. *Cf.* 15 U.S.C. §§ 1192, 1263, 2068. As a result, the CPSC recently launched Operation Safe Online Shopping, in which CPSC staff search online for products that violate federal safety standards or that are otherwise dangerous. Among the unsafe products it has found are flammable children's sleepwear that violate flammability standards, toys that violate safety standards, novelty lighters that are not child-resistant in violation of CPSC regulations, and children's jackets with drawstrings that can catch and strangle a child.[3]

Finally, as discussed in Part IV of the report, educational efforts are a critical part of any comprehensive strategy to protect consumers from online fraud. For instance, efforts to improve the reporting of complaints about Internet fraud, such as the Internet Fraud Complaint Center and the FTC's Consumer Sentinel website, can significantly enhance the ability of law enforcement and regulatory agencies to take effective action against Internet fraud schemes. The FTC and the Postal Inspection Service are working together to improve the sharing of complaint information to enable

[3] Through its website (www.cpsc.gov), the CPSC (1) educates the public about critical product safety issues; (2) provides a secure and efficient means by which consumers can report unsafe products; and (3) provides a medium through which manufacturers and distributors of consumer products can report substantial hazards associated with their products.

their investigators to respond to schemes while they are still in progress. The Postal Inspection Service has also modified its Fraud Complaint System and website to accept complaints filed via the Internet. And a major recent multi-agency fraud prevention campaign – Project "Know Fraud," which included mass mailings to consumers, a toll-free telephone number, videos, and a webpage (www.consumer.gov/knowfraud) – serves as an excellent example of how law enforcement agencies and the private sector can combine their capabilities and resources to educate consumers and prevent fraud.

4. Investigatory Challenges

Although existing substantive federal laws may generally be adequate to protect consumers against Internet fraud, certain aspects of the Internet may make certain fraud schemes more efficient in contacting victims in multiple jurisdictions or more effective in evading prompt detection and investigation by law enforcement.

The fact that the Internet transcends traditional jurisdictional boundaries, for example, presents special challenges in Internet fraud investigations:

> In 1996, Fortuna Alliance, a business headquartered in the United States, advertised on the Internet an investment opportunity, in which investors could earn as much as $5,000 per month, in perpetuity, after recruiting 300 new investors. After the Federal Trade Commission ("FTC") brought enforcement action against Fortuna Alliance and its principals, the head of the company left the country and transferred nearly $3 million of Fortuna's receipts to offshore bank accounts. Ultimately, the FTC returned $5.5 million from other Fortuna assets to 15,625 victims in 71 countries.
>
> In 1999, an individual in a Western European country accessed an online website based in Chicago, Illinois to purchase stereo speakers costing over $2,000. When the website merchant ran the individual's credit card through, it received authorization for the transaction and shipped the speakers. Subsequently, the true owner of the credit card disputed the charge, and the merchant had the full amount of the charge deducted from his merchant account. The merchant had no success in contacting the buyer abroad. Even if the buyer were identified and apprehended, prosecution of the perpetrator abroad would most likely have been not be worth the expense of trial, particularly if witnesses had to be flown from the U.S., given the relatively low (though significant to the merchant) monetary loss.

To investigate these types of Internet-facilitated schemes, law enforcement agents must deal with many of the same issues they would encounter in any international fraud investigation. These include the need to determine the validity of foreign addresses, the true identities of participants in the scheme, the location and content of banking information, and the location of suspects' assets.

The Internet, however, allows operators of an online fraud scheme to initiate, conduct, and terminate the scheme in a matter of hours, days, or weeks, in virtual anonymity, and operating rapidly across international boundaries, before traditional mechanisms such as mutual legal assistance treaties or letters rogatory (a letter request for assistance from one country's judicial authority to that of another country, *see, e.g.*, 28 U.S.C. § 1782) can be effectively employed to gather investigative information. The international reach of these schemes also increases the difficulty of carrying out restitution to victims of the schemes.

The global scope and impact of the problem therefore means that enforcement against all major forms of Internet fraud both domestically and internationally must be coordinated and effective. Through various international fora such as the G-8 and the International Marketing Supervision Network, as well as the Internet Fraud Initiative, federal law enforcement officials are moving to address several aspects of enforcement that warrant improvement.

A particular set of Internet-specific law enforcement challenges arises from the ability of criminals and hackers to obtain online and then use certain computer programs, such as Credit Master and Credit Wizard, that generate large volumes of credit card numbers. The sole purpose of these credit-card generator programs is to aid in finding particular credit card numbers that the program's user is not authorized to use, but that online merchants will accept. By generating a large enough group of card numbers that merchants will accept, participants in an online fraud scheme can make substantial fraudulent purchases of goods or services, or cause fraudulent billings for nonexistent goods or services, at the expense of the credit card company or the customers to whom the valid credit card numbers have been assigned. Although the use of such computer programs to further a fraud scheme would constitute credit card fraud in violation of 15 U.S.C. § 1644 and 18 U.S.C. § 1029, the relative ease with which such programs can be obtained increases the likelihood of such schemes being perpetrated.

In sum, law enforcement and regulatory authorities face significant challenges in investigating and prosecuting individuals responsible for Internet fraud schemes. The ability to gather and access evidence in a timely manner, for example, is crucial to the success of any investigation. There is little question that existing investigatory capabilities – including legal processes such as subpoenas, wiretaps, warrants, orders, and data-preservation letters (pursuant to 18 U.S.C. § 2703(f))[4] – are important tools in that effort. These legal authorities, however, can be of limited value to the extent some of them need to be updated to better reflect the realities of the online world (see Part III.D of the report).

In addition, to protect consumers online and prevent online fraud, cooperation and coordination with foreign law enforcement counterparts and industry must play an essential role.

---

[4] This provision requires a wire or electronic communications service provider, upon the request of any governmental entity, to "take all necessary steps to preserve records and other evidence in its possession pending issuance of a court order or other process," 18 U.S.C. § 2703(f)(1). Such records are to be preserved for 90 days, subject to a 90-day renewal period, *see id.* § 2703(f)(2).

In particular, efforts to improve assistance mechanisms internationally must continue to be developed (see Part III.E). The private sector must also continue to take responsibility and show leadership in efforts to address fraud on the Internet and to prevent offenders from evading law enforcement detection. For example, representatives of industry should consider evaluating their data retention policies so as to balance reasonable expectations of privacy with the need to protect consumers and merchants from perpetrators of fraud and other unlawful acts (see Part II.C). Efforts to improve the reporting of complaints about Internet fraud, such as the FTC's Consumer Sentinel and the Internet Fraud Complaint Center (see above), can also significantly enhance the ability of law enforcement and regulatory agencies to prevent and to take effective action against Internet fraud schemes.

5. Conclusions

The Internet has been used to perpetrate a variety of frauds. In response, the FTC, the Department of Justice, and other agencies have developed extensive programs to educate consumers to avoid becoming victims of online fraud. In addition, law enforcement agencies have used existing laws to actively investigate and prosecute those who are responsible for Internet fraud. Although existing federal substantive fraud laws are generally adequate, law enforcement agencies still face challenges in tracking online criminals, overcoming international barriers, and ensuring that key evidence is preserved. In addition, the failure of some individuals and companies to report Internet fraud weakens the effectiveness of law enforcement's efforts to combat Internet fraud.

APPENDIX C – ONLINE CHILD PORNOGRAPHY, CHILD LURING, AND RELATED OFFENSES

2. Nature of the Potentially Unlawful Conduct

The Internet, despite its many benefits, has unfortunately provided pedophiles with a new tool. Offering relative anonymity for sophisticated users and continuous access, the Internet has made it easy for child pornographers to distribute their materials and for pedophiles to lure and prey on children. As a result, child pornography is traded 24 hours a day in online chat rooms and in Internet Relay Chat channels,[1] and thousands of images of child sex abuse are available in easily accessible newsgroups.[2] In addition, pedophiles can lurk around chat channels and rooms and message boards and use e-mail to lure children for sex.

The prosecution of Internet-related child pornography and luring cases is increasing. The Department of Justice has found that prosecution of these cases has increased by 10 percent every year since 1995. Last year, the Department of Justice expects to have prosecuted over 400 such cases. Many of these cases are international in scope. For example, Operation Cheshire Cat, a joint investigation between the Customs Service and the English National Crime Squad, involved over 100 members of a major pedophile ring that operated in 21 countries.[3]

---

[1] Internet Relay Chat ("IRC") is a method for real-time discussion among multiple users. In each "channel" (discussion forum), participants are able to engage in the online equivalent of a party-line conversation, with response times limited only by one's typing speed. Discussion transcripts are not automatically created or stored unless an individual participant takes steps to do so. IRC channels, like mailing lists, may be either open to the public or by invitation-only. IRC channels can also be used for discussions that span multiple Internet sites. Many commercial services provide similar facilities (sometimes called "chat rooms") for their members. Other services (such as "ICQ" (I seek you) and "DCC" (direct channel chat)) permit private, one-to-one real-time chat activity.

[2] The Internet is also home to several thousand discussion groups known collectively as "Usenet." These discussion groups, also called "newsgroups," allow users to post public messages (including replies to earlier messages) on a variety of topics. Interaction does not take place in real time. Rather, communication more closely resembles a sequence of open letters than a multiparty telephone conversation.

[3] Operation Cheshire Cat has been the most complex investigation of an international child pornography trafficking organization to date. The investigation targeted an organization responsible for producing and trafficking in child pornography over the Internet, specifically on IRC channels, and involved the simultaneous execution of search warrants in 17 countries. With the assistance of the United Kingdom, 22 individuals have been prosecuted in the United States. Cooperation from Internet service providers ("ISPs") was crucial to this effort, for it was through records kept by ISPs that law enforcement agencies were able to identify the targets of their investigations.

3. Analysis of Existing Law

Although the growing number of child pornography and luring prosecutions is distressing, it also demonstrates the adequacy of existing federal laws designed to criminalize child pornography and other pedophile activities. Strong laws in these areas have made these prosecutions possible, and vigorous prosecution under these laws helps deter the illegal activity. In addition, various federal and state law enforcement agencies have collaborated to provide valuable resources and to share investigative techniques to protect children from predators.

Child pornography offenses are covered by 18 U.S.C. § 2251 *et seq*. These laws specifically include computers within the proscribed means of distribution and possession of child pornography. They specifically prohibit the production, transportation, receipt, or distribution of visual depictions that involve the use of a minor (any person under the age of 18) engaged in sexually explicit conduct, where the producer or distributor knows or has reason to know, that the depiction was or will be transported in interstate commerce or was created using a camera (or the like) that had traveled in interstate commerce. Computer graphic images – including computer or computer-generated images or pictures of a minor engaged in sexually explicit conduct; "morphed" images that appear to be (through computer manipulation) of a minor engaged in sexually explicit conduct; and images that are adults promoted as children engaged in sexually explicit conduct – are included within the definition of "visual depictions." 18 U.S.C. § 2256(5) and (8).[4]

Child luring is covered by 18 U.S.C. § 2422(b), which prohibits the use of any facility or means of interstate commerce to knowingly persuade, induce, entice, or coerce a minor to engage in criminal sexual activity or prostitution, or to attempt to do so. For example, in November 1999 an appellate court upheld the conviction of a defendant who pled guilty to one count of soliciting a minor for a sex act and three counts of transporting a depiction of a minor engaged in sexually explicit conduct. Using an online "screen name," the defendant engaged in a series of e-mail and real-time conversations with a government agent, whom the defendant believed to be a 14-year-old girl. During the conversations, the defendant repeatedly attempted to persuade the agent to meet him in a motel to engage in various sexual acts. In addition to these conversations, on three separate

---

[4] *See* United States v. Hilton, 167 F.3d 61, 65 (1st Cir.) ("Congress enacted the [Child Pornography Prevention Act] to modernize federal law by enhancing its ability to combat child pornography in the cyberspace era . . . . Lawmakers wished to improve law enforcement tools to keep pace with technological improvements that have made it possible for child pornographers to use computers to 'morph' or alter innocent images of actual children to create a composite image showing them in sexually explicit poses"), *cert. denied*, 120 S. Ct. 115 (1999); United States v. Acheson, 195 F.3d 645 (11th Cir. 1999); United States v. Fox, No. 1:99-CR-75, 1999 WL 976704 (E.D. Tex. Sept. 15, 1999). A recent court decision has, however, injected some uncertainty in this area. In December 1999, the U.S. Court of Appeals for the Ninth Circuit struck down portions of the Child Pornography Prevention Act of 1996, holding that the First Amendment prohibits Congress from enacting a statute that makes criminal the generation of images of fictitious children engaged in imaginary but explicit sexual conduct. *See* The Free Speech Coalition v. Reno, No. 97-16536, 1999 WL 1206649 (9th Cir. Dec. 17, 1999).

occasions, he trasmitted three different images of minors involved in sexually explicit conduct via his computer.

Another statute, 18 U.S.C. § 2423(a), prohibits a person from transporting a minor in interstate commerce with the intent to engage in criminal sexual activity with the minor or prostitution. A related provision, 18 U.S.C. § 2423(b), prohibits a person from traveling in interstate commerce, or conspiring to do so, for the purpose of engaging in criminal sexual activity with a minor. In September 1999, for example, a defendant in Wisconsin was sentenced to 15 months in prison, three years of supervised release, and a $2,000 fine after he pled guilty to a charge of traveling across state lines to engage in a sexual act with a minor whom he met in an online chat room. The defendant traveled from his home in Minnesota to the 14-year-old child's home in Wisconsin to engage in sexual activities with her.

In addition to these statutes, Congress recently enacted 18 U.S.C. § 2425 to provide additional protections for children online. This statute prohibits the use of a facility of interstate commerce, such as a computer connected to the Internet, to transmit information about a minor under the age of 16 for criminal sexual purposes. This statute is in response to a case from Illinois where an individual posted a 9-year old girl's name and telephone on the Internet, indicating that she was available for sex. This statute would apply any time a child predator communicates online with another child predator and provides personal information about a minor under 16 for criminal sexual purposes.

Congress has also permitted the Attorney General to delegate administrative subpoena authority to the FBI, the Criminal Division of the Department of Justice, and the United States Attorneys' Offices. *See* 18 U.S.C. § 3486A. Administrative subpoenas may be used to gain access to subscriber information from an Internet service provider ("ISP") during an online child pornography or child abuse investigation. This authority will significantly reduce the time needed to gain subscriber information from ISPs when an agent is seeking to identify a perpetrator who has used the Internet to lure a child. Congress has also required ISPs that become aware of an apparent violation of any federal child exploitation statute to report that information to a designated law enforcement agency. *See* 42 U.S.C. § 13032; *see also* 28 C.F.R. § 81.1 *et seq.* (requiring ISPs to report such violations to the National Center for Missing and Exploited Children, which in turn forwards complaints to designated federal law enforcement agencies).

Congress also has enacted other legislation to protect children from harmful material on the Internet. The Child Online Protection Act ("COPA") restricts the dissemination of "obscene" materials and materials "harmful to minors" over the world wide web. *See* 47 U.S.C. § 231.[5] The

---

[5] The statute provides an affirmative defense to liability, however, if the website attempts to screen minors from viewing the materials by requiring access through a credit card, debit card, or adult identification number. *See* 47 U.S.C. § 231(c). COPA's restriction on communications that are "harmful to minors" has been challenged by various commercial entities and civil liberties groups on First and Fifth Amendment grounds, and a district court has entered a preliminary (continued...)

statute also established a Commission on Online Child Protection to examine the extent to which current technological tools effectively help protect children from inappropriate online content. In 1999, Congress extended the deadline by which the commission was to submit its report to November 2000.

4. Specific Federal Initiatives

Federal, state, and local law enforcement agencies have all responded vigorously to child pornography and sexual exploitation on the Internet. In particular, the FBI, the Customs Service, the Postal Inspection Service, the Department of Justice's Child Exploitation and Obscenity Section ("CEOS"), and the National Center for Missing and Exploited Children ("NCMEC") have developed extensive programs and investigative and prosecutorial tools in response to child pornography and sexual exploitation on the Internet. In addition, the Department of Justice's Office of Juvenile Justice and Delinquency Prevention ("OJJDP") has played a leading role in coordinating cooperative efforts between federal, state, and local officials.

> *FBI's Innocent Images Initiative* – The FBI began the Innocent Images National Initiative in 1995 to address the problem of child pornography and child sexual exploitation facilitated through the use of the Internet and online services. Innocent Images is a proactive, intelligence-driven, multiagency investigative initiative. It is the central operation and case management system for all FBI investigations involving online child pornography and child sexual exploitation. The initiative focuses on individuals who indicate a willingness to travel for the purpose of engaging in sexual activity with a minor and those who produce or distribute child pornography. Cases evolving from the Innocent Images initiative have resulted in 358 convictions as of December 1999.
>
> *Customs' CyberSmuggling Center* – In August 1997, the Customs Service formed the CyberSmuggling Center, which (among other things) develops leads, tips, and complaints of child pornography and luring and forwards them to area offices for further investigation and case development. Some of these leads come from the Center's website, which received almost 6,000 tips between November 1997 and November 1998. The Center also conducts undercover operations to identify child pornography producers and distributors at the international level. These undercover operations have investigated operations on the World Wide Web, in newsgroups, in IRCs, in bulletin board services, and in commercial online services. Between November 1998 and September 1999, the Customs Service's child pornography investigations have resulted in 436 convictions.

---

[5](...continued)
injunction as to its enforcement with respect to such communications. *See* ACLU v. Reno, 31 F. Supp. 2d 473 (E.D. Pa. 1999), *appeal pending*, No. 99-1324 (3d Cir. argued Nov. 4, 1999).

Postal Inspection Service – Since the enactment of the Federal Child Protection Act of 1984, Pub. L. 98-292 (codified as 18 U.S.C. § 2251 note), the Postal Inspection Service has conducted more than 3,500 child exploitation investigations, resulting in the arrest and conviction of over 2,900 child molesters and pornographers. The Service increasingly is discovering that child molesters and pornographers are using computers, along with the mail, to find potential victims, to communicate with other criminals, and to locate sources of child pornography. In Fiscal Year 1998, nearly half of the Service's child exploitation cases involved computers. Among the Service's undercover operations are the placement of contact advertisements in sexually oriented publications, written contact and correspondence with subjects of investigations, development of confidential sources, and more recently, undercover contact with suspects via the Internet.

Child Exploitation and Obscenity Section, Department of Justice – CEOS has taken an active role in training federal prosecutors to handle child crime cases that were once mainly handled by local jurisdictions. The Section has sponsored several training seminars for federal prosecutors on the issues of child pornography and child exploitations. These training sessions have taught prosecutors and federal law enforcement agents the mechanics of computer hardware and software, the Internet, online investigative tools and techniques, and child exploitation laws. CEOS also offers U.S. Attorneys' offices litigation support through investigative advice, computer search warrant and indictment reviews, and joint prosecution of cases.

CyberTipline – NCMEC launched the CyberTipline in March 1998 to serve as a national online clearinghouse for tips and leads about child sexual exploitation (www.cybertipline.com). Mandated by Congress, the CyberTipline allows individuals to report online (and via a toll-free number) incidents of child luring, molestation, pornography, sex tourism, and prostitution. Since March 1998, the CyberTipline has received over 8,000 reports of child pornography alone.

Office of Juvenile Justice and Delinquency Prevention, Department of Justice – Pursuant to direct Congressional appropriations, OJJDP administers the Internet Crimes Against Children ("ICAC") Task Force Program[6] to help state and local law enforcement agencies respond to computer-facilitated child sexual exploitation offenses by creating regional clusters of forensic and

[6] The ICAC Task Force Program defines "Internet crimes against children" as the sexual exploitation of children by offenders using the Internet, online communications systems, or other computer technology. It encompasses crimes of child pornography and online solicitation of minors for sexual activity.

investigative expertise. Currently, ten agencies (covering 12 states) are operating, with an additional 16 sites slated to start online operations by April 2000.

4. Investigatory Challenges

Despite the general sufficiency of existing federal laws to combat child pornography and luring, and despite the extent to which law enforcement has gained effective new tools from the Internet and related technologies (such as CyberTipline noted above and the "investigative interests" database discussed below), law enforcement continues to face daunting challenges in its fight against online child pornography and pedophiles.

The ease with which sophisticated users can be anonymous on the Internet, the use of sophisticated encryption to conceal evidence of unlawful conduct on the Internet, and the need to coordinate international investigations and prosecutions, all hinder law enforcement agencies' ability to fight these types of crimes. In addition, ISPs may not generate records and data or retain them for a sufficient length of time to permit law enforcement agencies to respond to child pornography traffickers and predators. These challenges create barriers to the identification of perpetrators and to the gathering of other data and evidence for their prosecution.

One area in which law enforcement is having some success in responding to investigatory challenges posed by the Internet is the area of interagency coordination. Because the Internet renders conventional law enforcement boundaries virtually meaningless, one of the most important issues in general, but particularly in the area of child pornography and sexual exploitation investigations, is the effective coordination of interagency referrals and cases. Absent meaningful case coordination, law enforcement agencies are likely to conduct redundant investigations or disrupt undercover operations of other agencies. Consider the following examples:

> To avoid entrapment and to establish a suspect's predilection for sex with minors, a federal agent posing as a 13-year old girl develops a chat-room relationship with a middle-aged male. The agent becomes alarmed when the suspect postpones a meeting, citing weekend travel plans to meet another underage girl. Concerned for the potential victim's safety, the agent requests an arrest warrant for a lesser charge of conspiracy, while other agents attempt to identify the victim. One day later, the agent discovers that the "victim" was an undercover officer from another state.
>
> In another case, three federal agencies and one local law enforcement organization conduct parallel undercover operations targeting the same corporation. The independent investigations, aside from being redundant and a waste of resources, nearly result in the corporation learning prematurely of its target status and providing it an opportunity to destroy evidence or alter operating procedures.

OJJDP is addressing communication and coordination concerns by requiring ICAC Task Force agencies to register "investigative interests"[7] in a common database. Before conducting a full-blown investigation, ICAC Task Forces check this database to determine if a screen name or other potentially identifiable entity is targeted by another agency. If so, that agency is contacted to discuss the investigation and provided the additional information. If not, the inquiring agency registers its interest and proceeds with the investigation.

Nearly all ICAC Task Force investigations involve more than one jurisdiction and routinely require an extraordinary degree of multiagency collaboration. In anticipation of increased interagency referrals, federal, state, and local law enforcement agencies have expressed some concern about investigations that are initiated on the basis of information that may have been gathered through inappropriate investigative conduct or techniques by officers of another agency. In response to these concerns, OJJDP, with the input from the 10 original ICAC Task Force organizations and federal prosecutorial and law enforcement agencies, established ICAC Task Force operational and investigative standards. These standards address issues of information sharing, case coordination, undercover officer conduct, evidence collection, target selection, media relations, and supervision practices.

5. Conclusions

Many federal laws that have traditionally protected children – such as those used to combat child pornography and luring – also apply when individuals use the Internet to commit those offenses. Other laws have specifically been designed to deal with online child pornography and related crimes. Federal agencies, including the Customs Service and the Department of Justice, have developed numerous programs to protect children on the Internet. These have, for the most part, been successful. Despite the successes, law enforcement agencies still face numerous challenges in combating online child pornography and related crimes. The most daunting of these challenges are the anonymous nature of the Internet and the need for extensive coordination and communication between federal, state, and local law enforcement agencies.

[7] An investigative interest is established when there is a reason to believe that a screen name or other potentially identifiable entity has committed a crime or has engaged in a sequence of activities that is likely to lead to the sexual exploitation of a child.

APPENDIX D – INTERNET SALE OF PRESCRIPTION DRUGS AND CONTROLLED SUBSTANCES

1. Nature of the Potentially Unlawful Conduct

Over the past year, more and more consumers have purchased prescription drugs over the Internet. According to one recent study, online pharmacies sold more than $1.9 billion in prescription drugs, over-the-counter drugs, cosmetics, vitamins, toiletries, and other health and beauty products in 1999.[1] The ability to order prescription drugs over the Internet from online pharmacies can obviously provide significant societal benefits. Individuals who might otherwise have difficulty going to a "brick and mortar" pharmacy to obtain needed medications – such as persons with disabilities, the elderly, and those in rural communities – will surely benefit from the convenience of being able to order their prescription drugs online. Online sales are also likely to foster price competition for prescription drugs among licensed sellers. Any law enforcement initiatives must protect public health by deterring criminal and illegal pharmacy practices on the Internet and safeguard the privacy of confidential consumer information, yet avoid stifling the growth of the Internet generally or chilling its use as a communication medium, including its use for lawful commercial purposes.

In analyzing the legal issues surrounding online pharmacies, it is important to distinguish among three different types of online pharmacies.

> Some online pharmacies operate much like traditional "brick and mortar" or legitimate mail-order pharmacies. These online pharmacies use state-licensed pharmacists and require consumers to obtain valid prescriptions from licensed physicians before ordering drugs online. They verify that a licensed physician actually has issued the prescription to the patient before they dispense any drugs. These sites, like their physical counterparts, are covered by a comprehensive regulatory scheme that includes pre-market approvals, prescription drug designations, practitioner examinations, and pharmacy dispensing. This regulatory scheme, established under existing laws, has created a safety net to protect the American public from injuries resulting from unsafe drugs, counterfeit drugs, and improper prescribing and dispensing practices.

---

[1] *See* Online Pharmacy Sales Top $1.9 Billion, E-Commerce Times, Jan. 13, 2000. Still, "Internet prescription sales in 1999 represented a small slice – about $160 million – of the $101 billion U.S. market," according to Forrester Research, an Internet research firm. *See* Laura Johannes, Competing Online, Drugstore Chains Virtually Undersell Themselves, Wall St. J, Jan. 10, 2000, at B1. By 2004, however, Forrester Research estimates that prescription drug sales over the Internet will account for $15 billion. *See* Online Healthcare Expected to Reach $370B by 2004, E-Commerce Times, Jan. 4, 2000.

Other online pharmacies offer to "diagnose" a patient online, to "prescribe" the medication, and to distribute it without a licensed prescriber (such as a physician) ever physically seeing the patient. These websites typically use an online medical questionnaire, which asks for the patient's health profile, current medication, and medical history (see sidebar on Online Pharmacies – Potential Health Risks). Based on this questionnaire, a prescriber affiliated with the website "diagnoses" the patient's ills and prescribes medication, which the website's pharmacy then distributes. These websites may appeal to consumers who wish to purchase "lifestyle" drugs (such as those used for erectile dysfunction or hair loss), but do not want the inconvenience or embarrassment that might accompany a request to a doctor, or who might wish to resell these drugs.

Still other online pharmacies are websites that allow consumers to purchase prescription drugs without any type of prescription. These websites may also appeal to consumers who wish to obtain certain medications without first obtaining a prescription. It is also possible that consumers who have been told by doctors that they should not take certain drugs may try to circumvent the system by going online and buying the drugs that doctors have denied them.

Online pharmacies that dispense prescription drugs based solely on an online questionnaire or that do not require a prescription at all pose a significant risk to public health for three reasons. First, they circumvent the traditional protections built into the doctor-patient relationship, such as when a doctor requires a patient to undergo a physical examination to make a diagnosis and identify drug allergies or physical ailments that make taking certain drugs dangerous to the patient's health. Second, the inability of consumers to confirm the legitimacy of online pharmacies, many of which might be located overseas, increases the risk that drugs are placebos, mislabeled, or counterfeit, and the inability to confirm the authenticity of the doctors associated with them likewise offers little comfort regarding the adequacy of medical review. Finally, because the Internet can be an anonymous medium, some online pharmacies might be nothing more than scams, collecting credit card numbers and cash, but providing no products. In the physical world, consumers have certain protections against the fraudulent sale of prescription drugs (*e.g.,* consumers can physically enter a store and see who is selling a drug or can receive approval from their insurance company to use certain mail-order services). In the cyberworld, such protections are not as obviously present.

An increasing number of illegal drug traffickers (whether they deal in cocaine, heroin, MDMA, LSD, marijuana, controlled substances such as anabolic steroids, or precursor chemicals that are needed to manufacture illicit drugs) are also using the Internet. With portable computers and online connections, illegal drug traffickers can transmit text, audio, and video; track shipments; and engage in financial transactions virtually anywhere in the world. In short, the Drug Enforcement Administration ("DEA") and other drug enforcement officials are increasingly finding that illegal drug traffickers are turning to innovative technologies to conduct their businesses, disguise their activities, and avoid law enforcement scrutiny.

Online Pharmacies – Potential Health Risks

The potential health risks created by online pharmacies that offer online diagnoses and prescriptions are best illustrated by example.

> Viagra™ is a commonly sold prescription drug on the Internet. It is indicated for the treatment of erectile dysfunction, which may be a symptom of more serious diseases, including heart disease. Without a physical examination, a patient's underlying heart disease or other condition may not be detected, with potentially fatal consequences. A recent survey of websites selling Viagra™ found that 45 percent of them provided no information about contraindications, *e.g.,* concomitant use of nitrates, and 56 percent provide no information about other risk factors. *See* K. Armstrong, J.S. Schwartz & D.A. Asch, Direct Sale of Sildenafil (Viagra) to Consumers over the Internet, 341 New Eng. J. Med. 1389 (1999). Hearings before the House Subcommittee on Oversight and Investigations, Committee on Commerce, also revealed numerous examples of websites selling Viagra™ to consumers who were at risk of heart disease.
>
> Prescription diet drugs are also commonly sold over the Internet. Suppose an anorexic woman who seeks such a drug fills out an online questionnaire, and in the section on height and weight, the woman states that she is 5'9" and weighs 280 lbs. when, in fact, she weighs only 80 lbs. She also fails to mention on the questionnaire that she is being treated for anorexia nervosa and depression with suicidal thoughts. A "doctor" reviews the questionnaire, but does not bother to call her primary care physician. Based on the information contained in the questionnaire, the "doctor" prescribes the diet drug. A week later, the woman is rushed to the hospital for attempting suicide by overdosing on the drug.

2. Analysis of Existing Law

The Federal Food, Drug, and Cosmetic Act ("FDCA"), 21 U.S.C. § 301 *et seq.*, prohibits the manufacture and distribution of misbranded and adulterated drugs, requiring them to be labeled accurately and manufactured and properly handled in ways that prevent contamination or misuse. Congress established the regulatory scheme that currently governs the sale of prescription drugs in 1951 to protect the public from abuses arising from the sale of potent prescription drugs and to relieve retail pharmacists from burdensome and unnecessary restrictions on the dispensing of over-the-counter drugs. *See* 21 U.S.C. § 353(b)(1). That regulatory scheme relies largely on two health professionals – a physician and a pharmacist – to protect patients from the knowing or accidental misuse of medicines that are toxic or that have the potential for causing harm.[2]

[2] To help ensure that these health professionals are knowledgeable about their patients, (continued...)

Accordingly, drugs that are considered prescription drugs under the FDCA may be dispensed only with a valid prescription of a practitioner licensed to administer the drug. *See* 21 U.S.C. § 353. A prescription drug is considered "misbranded" if it is not dispensed pursuant to a valid prescription in accordance with 21 U.S.C. § 353(b)(1). Introduction or delivery for introduction of misbranded drugs into interstate commerce violates the FDCA. *See* 21 U.S.C. § 331(a). Legal action to curtail the distribution of misbranded drugs – including distribution of drugs without a valid prescription – may be brought criminally or civilly. For a felony conviction, the government must establish that the defendant acted with intent to defraud or mislead or that the defendant is a repeat offender. *See* 21 U.S.C. § 333(a). Civil cases and misdemeanor prosecutions do not require proof of intent to defraud or mislead.

An online pharmacy that provides prescription drugs without a prescription – the third category of online pharmacies noted above – would plainly be in violation of the requirements of section 353(b)(1). For online pharmacies that offer online diagnosis, prescription, and distribution of medication – the second category of online pharmacies noted above – the issue is whether the online interaction results in a valid "prescription" under 21 U.S.C. § 353(b). That issue may depend on state law. Traditionally, the licensing and regulation of doctors and pharmacies have been the responsibility of the states.[3] For a prescription to be valid under this federal provision, however, there is a strong argument that it needs to be based on a legitimate doctor-patient relationship. For example, with the assistance of FDA, the Department of Justice has successfully prosecuted doctors who "prescribed" steroids (which were regulated at the time as prescription drugs, rather than controlled substances, as they are now) without establishing legitimate doctor-patient relationships with their customers. And the Federation of State Medical Boards has taken the view that "[w]ebsites that offer prescription drugs based solely on an electronic medical questionnaire are a threat to public safety and physicians who participate in such offerings clearly fail to meet an

---

[2](...continued)
Congress in effect prohibited the practice of "diagnosis by mail"– *i.e.,* the issuance of a prescription on the basis of a form completed by a patient and mailed to a business that employs a doctor to review such forms. *See* 21 U.S.C. § 353(b)(2) (excluding "any drug dispensed in the course of conduct of a business of dispensing drugs pursuant to diagnosis by mail" from exemptions to the requirement that prescription drugs bear adequate instructions for use); Proposed Amendments to Section 503(b) of the Federal Food, Drug, and Cosmetic Act of 1938: Hearings before the Subcomm. on Health of the Senate Comm. on Labor and Public Welfare, 82d Cong. 36-39, 185, 202 (1951); S. Rep. No. 946, at 7 (1951).

[3] Generally, state boards of medicine and pharmacy prescribe rules governing those disciplines within their respective states. *See, e.g.,* Va. Code, tit. 54.1, subtit. III, ch. 29 (requiring practitioners of medicine and related healing arts to have a license from state Board of Medicine, which is given authority to regulate those practitioners); Va. Code, tit. 54.1, subtit. III, ch. 33 (requiring pharmacists to have a licence from state Board of Pharmacy, which is given authority to regulate pharmacies).

acceptable standard of care."[4] If a prescription is not valid, then the online pharmacy may be found to be distributing "misbranded" medication in violation of the FDCA.[5]

Some of the drugs available online (or the subject to drug trafficking) are controlled substances. The Controlled Substances Act prohibits the knowing or intentional unauthorized manufacture, distribution, possession, or intent to manufacture any controlled substance; it also requires that all persons who import, export, manufacture, distribute, or dispense a controlled substance in the United States obtain a registration. *See* 21 U.S.C. §§ 822, 829, 841, 958. Because the statute regulates conduct in a technology-neutral way, it applies to online pharmacies and other websites that offer or dispense controlled substances.[6]

The registration of all authorized domestic handlers of controlled substances in the United States serves as the basis for a "closed" system of distribution – only those properly authorized or registered may obtain controlled substances from another registrant or may import them, and those licensed and authorized to dispense such substances to the ultimate user or consumer are mandated to do so pursuant to legitimate medical and pharmacy practices as defined by state law. Indeed, the DEA has issued a regulation that defines "prescription" in a way that may make it impossible to issue a valid prescription for controlled substances on the basis of an online "diagnosis" as a regular course of business (though online diagnoses in emergency situations might still be permissible). *See* 21 C.F.R. § 1306.04.

Another potential avenue for enforcement involves the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 *et seq.* The FTC Act protects consumers from unfair or deceptive acts or practices, including the false advertisement of drugs, *see id.* §§ 45(a), 52. Actions to enjoin violations of the FTC Act may be initiated administratively or filed in federal district court, *see id.*

---

[4] Letter from James R. Winn, M.D., Executive Vice President, Federation of State Medical Boards of the United States, Inc., to Nelson Peacock, Office of Intergovernmental Affairs, U.S. Dep't of Justice (Nov. 1, 1999). Similarly, the FDA, the National Association of Boards of Pharmacy, and the Federation of State Medical Boards have noted in a joint statement that "[a] health care practitioner who offers a prescription for a patient the practitioner has never seen before and based solely on an online questionnaire generally has not met the appropriate medical standard of care." Principles of Understanding on the Sale of Drugs on the Internet (July 28, 1999).

[5] Though not addressed in this report, the sale of veterinary prescription drugs sold over the Internet also raises many of the same issues. The FDCA provides that veterinary prescription drugs must be sold and used through a prescription that is based on a legitimate veterinarian-patient relationship. These drugs are often used in food-producing animals, and without a veterinarian's oversight, they may be misused, resulting in drug residues that are potentially harmful to humans.

[6] Another relevant portion of the statute is 21 U.S.C. § 863, which makes it illegal for a person to sell or offer for sale drug paraphernalia, to use any facility of interstate commerce to transport drug paraphernalia, or to import or export drug paraphernalia. These prohibitions also apply in a technology-neutral way to cover conduct involving the use of the Internet.

§§ 45(b), 53. Many online pharmacies make important representations to consumers on their websites. For instance, claiming that a properly licenced physician will review the online questionnaire would be such a representation, as would a representation that a product is safe. Websites may represent, falsely, that medical information collected from consumers will be kept confidential or that an online consultation is equivalent to a physical examination. To the extent such representations are false or deceptive, the online pharmacy would be violating the FTC Act, thereby subjecting the website operator to a civil enforcement action.

Federal law enforcement may also look to the federal mail and wire fraud statutes whenever an online or other pharmacy defrauds consumers. Whether such a suit would be criminal or civil, under 18 U.S.C. § 1345 or the FDCA, would depend on the precise facts of the case and the evidence of fraudulent intent. Schemes involving the sale of drugs or health products over the Internet may also violate other related federal criminal laws. Some websites offer to bill private or public health care programs or insurers for a "doctor's" advice or for the price of the drug or product itself. False representations to an insurer to obtain payment can implicate both federal criminal and civil laws.

Based on the above analysis, existing federal law appears generally adequate to encompass the unlawful sale of prescription drugs over the Internet. The same substantive legal requirements that apply to the sale of prescription drugs from the corner pharmacy, by mail order, or by the telephone also apply to such sales over the Internet. The Internet simply provides another means of communication.

3. Investigatory Challenges

Even if existing federal *substantive* law is adequate, unlawful online pharmacies raise a host of difficult investigatory issues. Solutions are complicated given the fact that the diagnosis of medical problems and the sale and distribution of prescription drugs domestically are regulated by different federal and state agencies (as discussed below, the situation is even more complicated when foreign websites are involved). The federal government, through federal statutes such as those described above, has substantial jurisdiction over the illegal sale of prescription drugs. At the same time, states have jurisdiction over doctors and pharmacists practicing within their borders.

State regulators, however, face many significant challenges to enforcing existing state laws relating to the practice of prescribing and dispensing medicine against online practitioners. In many cases it can be difficult, without extensive time and resources, even to identify the name, location, and state of licensure or registration of the physicians, pharmacists, and website operations involved. Even when relevant parties can be identified and located, it can be difficult and costly for a state to pursue enforcement action against an out-of-state physician or pharmacist. Even if such an action were successful, the website operator would not be precluded from continuing to operate in other states.

There have been a number of proposals to address this investigatory challenge:

> The Administration recently announced a new initiative to protect consumers from the illegal sale of prescription drugs over the Internet. In addition to

increasing existing penalties and investigative resources and launching a new public education effort, the initiative would establish new federal requirements for online pharmacies to ensure that they comply with relevant state and federal laws. These requirements, the details of which are undergoing interagency review, might include disclosures or certifications regarding the identity of pharmacists or other relevant health care professionals employed by the website and the states in which they are licensed.[7]

In July 1999, the FTC proposed that websites that offer to sell prescription drugs must disclose information such as the name, address, and telephone number of the pharmacy that will dispense the prescription and the states where the pharmacy is licensed or registered to do business; the name, address, and telephone number of each physician providing online prescribing services and the states where each physician is licensed or authorized to practice medicine; the name, address, telephone number, and principal officers of the online business offering the prescription drugs; and the states from which the website will accept orders for prescription drugs.[8]

In August 1999, Congressman Klink introduced the Internet Pharmacy Consumer Protection Act, H.R. 2763, 106th Cong. (1999), which would require online pharmacies to provide on their websites identifying information, such as the name of the principal practitioner, the address and telephone number of the principal place of business, and the states in which the pharmacy and pharmacists are licensed. If the website provides medical consultations for prescriptions, it would also have to disclose the names and licensing information of the prescribers. The proposed legislation would authorize FDA to enforce these requirements.

These proposals generally complement existing federal laws regarding the sale of prescription and unapproved drugs. In the offline world, consumers are assured of the safety and suitability of the drugs that they take not only because the drugs must be prescribed by a licensed physician, but also because they must be dispensed by a licensed pharmacy. When, for example, an offline consumer walks into a brick-and-mortar pharmacy to have a prescription filled, he or she knows the identity and location of the pharmacy, and the pharmacy's license on the wall provides visual assurance that it meets certain health and safety requirements in that state. In the online

---

[7] This certification proposal could be modeled on a voluntary certification program offered by the National Association of Boards of Pharmacy, in which the organization verifies the licensure of online pharmacies and provides a "Verified Internet Pharmacy Practice Site" seal of approval to sites that meet its standards.

[8] *See* Drugstores on the Net: The Benefits and Risks of Online Pharmacies: Hearings Before the Subcommittee on Oversight and Investigations, House Comm. on Commerce, 106th Cong. (1999) (statement of the FTC).

world, existing law requires a consumer to have a valid prescription from a licensed physician before a prescription drug can be dispensed, but does not provide a mechanism for identifying the online pharmacy or verifying that it is properly licensed. These proposals (and variations thereof) therefore fill a gap in the existing regulatory structure to protect consumers from illegitimate online pharmacies – *i.e.*, those that seek to operate without complying with relevant state and federal laws.

In addition, as noted above, the proposals address an important investigatory need. Sites that operate without the required disclosures or certifications would be subject to sanctions. The failure to disclose or to display proper certification would provide investigators with a rapid and coordinated way in which to identify illegitimate online pharmacies. Penalties for false disclosures or certifications would deter such misrepresentations, and having a single enforcement mechanism would permit rapid and coordinated investigations, while retaining traditional state authority to regulate pharmacies.

In the meantime, several federal and state law enforcement agencies are already working together to create coalitions to combat the illegal sale of online pharmaceuticals. These alliances preserve traditional jurisdictional boundaries between federal and state law enforcement, while targeting illegal online pharmacies that threaten public health and safety.

A good example of a joint federal-state alliance is that entered into in August 1999 by the Kansas Attorney General's Office and the U.S. Attorney's Office for the District of Kansas. In addition to these two offices, the alliance includes representatives from the Kansas Pharmacy Board, Kansas Board of Healing Arts, Consumer Protection Division, the Medicaid Fraud and Abuse Division and the Food and Drug Administration's Office of Criminal Investigations. In this coalition, state authorities have taken the lead in dealing with online pharmacies that may not meet state regulations but are attempting to offer legitimate pharmaceutical services. The Kansas authorities have found that these entities will generally conform their conduct to meet state regulations after notification. For its part, the U.S. Attorney's Office is assisting the state with the identification of individuals, including doctors, responsible for illegal online pharmacy drug sites. In turn, Kansas state authorities are taking legal action against doctors, websites, and pharmacies that dispense prescription drugs over the Internet in violation of state law on grounds that "prescriptions" issued based on online interaction are not valid.

In addition to combating the unlawful sale of prescription drugs from domestic website operators, law enforcement agencies are also examining how to stop foreign Internet sites from selling prescription drugs that are then illegally imported into the United States. The United States continues to seek and obtain the cooperation of foreign governments in enforcing U.S. laws, including those that pertain to prescription drugs. Foreign sales of pharmaceutical controlled substances at the retail level into the United States via the Internet violate the United Nations Convention Against Illicit Traffic in Narcotics and Psychotropic Substances of 1988 as well as the Controlled Substances Act, 21 U.S.C. §§ 951-971. Virtually all countries that would be foreign sources for such substances are parties to the U.N. convention.

Although international awareness and cooperation on fighting crime has grown, we must continue to resolve philosophical differences between countries on combating the sale of illegal

goods online and also to develop practical ways to enforce our laws. For example, the focus of our concern with prescription drugs from foreign countries is not necessarily with the Internet aspect of the sale, but with the illegal importation and distribution of those drugs in the United States. One way to stop these sales might be for law enforcement agencies in the United States, in particular, the Customs Service and FDA, to work with their counterparts in countries with online prescription firms to prevent the shipping of the drugs into the United States.

The Customs Service's CyberSmuggling Center is, for example, actively working with Customs attaché offices and their foreign counterparts to identify and target online pharmacies located outside the United States that are shipping prescription drugs and controlled substances into the United States. Customs' International Mail Facilities are successfully stopping parcels entering the United States. Upon a determination by FDA that the drugs are in violation of law, the parcels are seized and referred for investigative follow-up. The Customs Service seized 9,725 packages with prescription drugs last year, over four times as many as were seized in 1998.[9] Despite these efforts, the Customs Service and the FDA would require a substantial increase in resources and personnel as a practical matter to stop all, or even most, illegal prescription drugs from entering the country.

4. Conclusions

Apart from new legislative efforts to require online pharmacies to make certain disclosures or to obtain appropriate certifications, existing substantive federal law (for now at least) appears to be adequate. The same federal legal requirements that apply in the physical world apply to the online sale of prescription drugs and illegal drugs. There are nevertheless numerous issues that create investigative difficulties for law enforcement. There are jurisdictional issues, as both federal and state officials have jurisdiction over the activities relating to the sale of prescription drugs. In addition, international issues have arisen, because many websites that offer drugs (approved and unapproved in the U.S.) are located outside the country. And, there is a pressing need for coordination of enforcement policies and initiatives among a variety of federal, state, and local entities. It is crucial that law enforcement agencies – at all levels – receive the training, funding, and other support necessary to conduct investigations into online pharmacies that threaten the public health without impairing those that provide prescription medication in a safe, legal, and convenient way.

[9] *See* Robert Pear, Online Sales Spur Illegal Importing of Medicine to the U.S., N.Y. Times, Jan. 10, 2000, at A1.

APPENDIX E – INTERNET SALE OF FIREARMS

1. Nature of the Potentially Unlawful Conduct

The Internet can provide a means for young people or other prohibited individuals, such as felons, fugitives, and drug addicts, to obtain firearms. This is because the Internet provides a convenient forum for the advertisement and sale of guns by non-licensed individuals who, unlike federal firearms licensees ("FFLs"), are not required to conduct background checks on prospective purchasers or maintain records of sales. The firearms eligibility background checks that are required by the Brady law have proven extremely effective in preventing guns from falling into the wrong hands, stopping more than 400,000 criminals and other prohibited people from obtaining guns from FFLs since 1993. Young people and criminals who are turned away by licensed dealers may turn to the Internet to obtain guns. The Internet, therefore, is one more forum (in addition to gun shows and newspaper classified advertisements) where many guns can be sold nearly anonymously and without background checks. As a result, these guns often cannot be effectively traced back to the purchaser if they are later used in crimes.

Because the Internet provides an inexpensive means to offer items for sale through on-line classified advertisements, auction sites, and on-line marketplaces, the Internet also makes it easy for private individuals to violate the law by dealing in firearms without obtaining the requisite license. (In response to this problem, some e-commerce merchants, such as some Internet auction sites, do not permit postings that involve firearms transactions on their websites.) In addition, the Internet makes it easier for such sales to occur without either the buyer or seller being made aware of the applicable legal requirements.

Another type of unlawful conduct that may occur on the Internet involves possible violations of the restrictions on interstate sales of firearms that are imposed by federal law. Because offers for sale posted on the Internet will be accessible to people all across the country – and indeed all over the world – there is a strong possibility that prohibited interstate or foreign sales will occur.

Finally, there is the possibility that some FFLs will violate federal law to take advantage of the commercial opportunities presented by the Internet. For example, FFLs are required to examine identifying documents of the purchaser and may not sell guns to persons who are prohibited, underage or, in the case of handguns, do not reside in the state in which the FFL is licensed. The Internet may create a temptation on the part of FFLs to circumvent any and all of these requirements, as well as recordkeeping requirements, because of the potential profits that can be earned from online sales.

2. Analysis of Existing Law

Gun sales on the Internet are covered by existing laws and regulations governing commerce in firearms. The principal federal law that applies is the Gun Control Act of 1968, which requires those who "engage in the business" of importing, manufacturing, or dealing in firearms to obtain a federal firearms license from the Secretary of the Treasury. *See* 18 U.S.C. § 922(a)(1). Such a

license entitles an FFL to ship, transport, and receive firearms in interstate or foreign commerce. Having a license also imposes obligations on an FFL. For example:

> FFLs must maintain records of all acquisitions and dispositions of firearms and comply with all State and local laws that apply to the transfer of firearms.
>
> FFLs must positively identify gun purchasers by examining a government-issued photographic identification, such as a driver's license.
>
> FFLs must comply with the Brady law before transferring a handgun or a long gun to a non-licensee. The Brady law requires an FFL to contact the National Instant Criminal Background Check System ("NICS") before transferring a firearm to any non-licensed person to determine whether the receipt of a firearm by the prospective purchaser would violate federal or state law.

The Gun Control Act prohibits an FFL or any non-licensed transferor from transferring firearms to persons the transferor knows or has reason to believe are disqualified from receiving or possessing a firearm. *See* 18 U.S.C. § 922(d). The prohibited categories include: convicted felons or persons under indictment for a felony (persons under indictment may possess firearms, but may not receive additional firearms while under indictment); fugitives from justice; drug addicts or users of illegal drugs; persons who have been adjudicated mentally defective or involuntarily committed to a mental institution; illegal aliens or non-immigrant aliens; persons dishonorably discharged from the military; persons who have renounced their U.S. citizenship; persons under certain types of civil protection orders; and persons convicted of a misdemeanor crime of domestic violence. *See id.* In addition, subject to certain exceptions, persons under 18 may not possess handguns, and FFLs may not sell or deliver rifles or shotguns to persons under 18 years of age or handguns to persons under 21 years of age. *See* 18 U.S.C. § 922(b)(1), (x)(2) & (x)(5).

In addition to the regulation of licensed firearms dealers, the Gun Control Act also governs the activities of licensed firearms collectors, for whom the Internet undoubtedly provides a convenient and legitimate means to communicate and trade with other collectors. Collectors must obtain a collector's license if they seek to ship, transport, or receive firearms classified as "curios" or "relics" in interstate or foreign commerce. *See* 18 U.S.C. §922(a). Licensed collectors also have recordkeeping obligations, but they are not required to conduct Brady background checks in connection with transfers.

As noted above, the requirements for licensing apply only to those individuals who are "engaged in the business" of dealing in firearms. This condition exempts from the licensing requirement many individuals who buy and sell guns as a hobby or not as a means of livelihood or profit. *See* 18 U.S.C. § 921(a)(21)(C); 18 U.S.C. § 922(a). Because individuals who are not "engaged in the business" may lawfully sell firearms without becoming a licensee, these individuals do not have the same requirements as FFLs to verify identities, to conduct Brady background checks, or to maintain records of the transactions.

There are also limitations placed on the interstate transfer of guns. Under the Gun Control Act, it is unlawful for an FFL to sell a handgun to a resident of another state. *See* 18 U.S.C. § 922(b)(3). A person can arrange, however, for the transfer of a handgun from an out-of-state dealer to an in-state dealer who conducts the background check and who otherwise fulfills the obligations of a licensee transferring the gun. (Long guns are excepted from this general prohibition; they can be bought by individuals from an out-of-state dealer if the purchaser appears in person at the out-of-state dealer's place of business.)

Under current law, an FFL or non-licensed transferor is prohibited from shipping firearms across state lines to non-licensees. *See* 18 U.S.C. § 922(a)(2). (Different rules apply to long guns: individuals may ship long guns across state lines to themselves in their state of residence, and an FFL may transfer a rifle or shotgun "over-the-counter" to a nonresident of the state as long as the buyer and FFL meet in person to accomplish the transfer and if the transfer is legal in both of the states where the buyer and FFL reside.)

In addition to federal law, many states have laws prohibiting the transfer of firearms to enumerated classes of persons. Several states restrict the private sale of firearms by unlicensed persons and require all transfers to be made through a licensee, who can perform a background check and retain records of the sale. Other states require persons who wish to purchase a firearm to obtain a permit or to wait to receive the firearm until the expiration of a mandatory waiting period.

3. Investigatory Challenges

Although the existing framework of federal firearms laws applies to transfers of firearms on the Internet, the Internet does present some unique problems. First, the Internet provides opportunities for illegal firearms commerce that will be difficult for law enforcement to detect. Unlike the classified section of a newspaper, which can easily be obtained and reviewed by law enforcement to determine whether a person is engaging in the business without a license, the Internet provides people with a means to advertise guns for sale on message boards, through e-mail, in chat rooms, or other websites that will be difficult to find and may even be inaccessible to law enforcement.

Second, unlike gun sales from a physical location, such as a gun store or a booth at a gun show, the sale of guns on the Internet does not require a fixed location or a specific duration. This can make it difficult to monitor the activities of the seller (*e.g.,* dealing by unlicensed persons) as well as the buyer (*e.g.,* sales to prohibited persons). The enforcement activities of the Bureau of Alcohol, Tobacco and Firearms ("ATF") often depend on its ability to conduct inspections of licensed dealers and to review records of transactions. Internet sales – which do not occur at fixed physical locations – can make these tasks more difficult.

Determining how to meet the challenges of firearms sales on the Internet raises important issues regarding the sale of firearms and commercial speech. There have been legislative proposals, such as S. 637 (introduced by Senator Schumer in March 1999), to regulate firearms transactions on the Internet by requiring website operators who allow advertisements of firearms sales on their sites to obtain a license, and to prohibit buyers and sellers who access a licensed website from identifying

themselves to each other (to keep them from evading the licensed operator by directly contacting one another). These proposals would require any website operator who allows guns to be offered for sale on the operator's website to act as an intermediary to process the transaction and ensure that the buyer and seller do not attempt to circumvent the legal requirements that apply to the transaction. These proposals, however, raise questions about the propriety of treating one medium for regulation in a way that is inconsistent with the way other media (*e.g.*, newspapers) are treated.

Moreover, we currently lack reliable information regarding the nature and prevalence of unlawful sales of guns on the Internet. ATF has relied upon traditional investigatory methods to obtain information about specific illegal Internet sales of firearms, including information received from concerned citizens, informants, and cooperating defendants. ATF is in the process of establishing a pilot project to determine the nature and scope of unlawful Internet activity relating to firearms, including the extent of sales to prohibited persons, dealing without a license, sales of assault weapons and other prohibited firearms, illegal shipment or transportation, and illegal interstate sales. In addition, ATF is holding discussions with several Internet service providers on how to prevent the illegal sale of firearms to juveniles over the Internet.

4. Conclusions

Gun sales on the Internet are covered, as a matter of substantive law, by existing federal laws and regulations governing commerce in firearms. The challenges facing law enforcement with the sale of firearms online include: (1) problems detecting illegal firearms commerce; (2) difficulties identifying sellers and buyers of illegal firearms; and (3) lack of reliable information regarding the nature and scope of unlawful sales of firearms on the Internet.

APPENDIX F – INTERNET GAMBLING

1. Nature of the Potentially Unlawful Conduct

The growing availability of the Internet and other emerging technologies has had a dramatic impact on gambling businesses. Studies estimate that between 1997 and 1998, Internet gambling more than doubled, from 6.9 million to 14.5 million gamblers, with revenues more than doubling from $300 million to $651 million.[1] A recent estimate reported 300 Internet gambling sites in operation.[2] This rapid rate in the growth of Internet gambling is alarming and has caused several problems for federal, state, tribal, and local governments in the enforcement of their gambling laws.

First, the Internet is attractive to organized crime groups that operate gambling businesses, because it allows virtually instantaneous and anonymous communication that can be difficult to trace to any particular individual or organization. There is also the possibility of abuse by unscrupulous gambling operators. The ability for operators to alter, move, or entirely remove sites from the Internet within minutes makes it possible for dishonest operators to take credit card numbers and money from deposited accounts and close down. Operators may tamper with gambling software to manipulate games to their benefit. Unlike the highly-regulated physical world casinos, assessing the integrity of Internet operations is difficult. Gambling on the Internet also may provide an easy means for money laundering, as it provides criminal anonymity, remote access, and access to encrypted data.

Second, the anonymous nature of the Internet also creates the danger that access to Internet gambling will be abused by underage gamblers. Gambling businesses have no surefire way of confirming that gamblers are not minors who have gained access to a credit card and are gambling on their websites. The government has received numerous complaints from concerned and affected citizens regarding this problem.

Third, because the Internet provides people with the opportunity to gamble at any time and from any place, Internet gambling presents a greater danger for compulsive gamblers and may cause severe financial consequences for the player and those dependent on the player's resources (*e.g.*, dependent children).

---

[1] National Gambling Impact Study Comm'n, Final Report 2-15 (1999) ("NGISC Final Report") (citing research conducted by gambling industry analysts at Christiansen/Cummings Associates).

[2] *See* Internet Gambling: Hearings Before the Subcommittee on Technology, Terrorism, and Government Information, Senate Comm. on the Judiciary, 106th Cong. (1999) (statement of Ohio Attorney General Betty Montgomery).

As the National Gambling Impact Study Commission[3] recently found:

> Internet gambling is raising issues never previously addressed and exacerbating concerns associated with traditional forms of gambling. While preventing underage gambling and reducing problems associated with problem and pathological gambling are concerns for all forms of gambling, reducing these concerns is particularly challenging for Internet gambling. The Internet provides the highest level of anonymity for conducting gambling to date. . . . Screening clients to determine age or if they have a history of gambling problems is difficult at best.[4]

These problems are exacerbated by the international scope of the Internet. Although the United States has determined that there is a strong law enforcement priority to prohibit Internet gambling, other countries have chosen to allow unrestricted Internet gambling (as certain countries in the Carribean have done) or, in the alternative, to regulate betting and wagering on the Internet. The United States government, in its assessment of existing and needed laws, must adopt solutions that do not interfere with the operation of these lawful foreign gambling operations, while protecting its citizens from the transmission of bets or wagers into or from the United States.

2. Analysis of Existing Law

The federal government has traditionally deferred to the states to regulate or prohibit gambling activities, devoting its attention to gambling activities involving criminal matters (*e.g.*, organized crime and fraud) or matters involving interstate or foreign commerce. States, in turn, have considered their communities' moral beliefs, evidence of the social impacts of gambling, and concerns about associated criminal activities, in deciding how to address gambling. In the late 1950s, however, states discovered that the telephone and other communications facilities were transforming gambling into more of a federal issue. Illegal bookmaking operations, often run by organized crime groups, were using these technologies to transmit gambling information rapidly between states and to and from foreign locations.

In view of the growing use of such technology by bookmaking operations in furtherance of their criminal activities, then-Attorney General Robert F. Kennedy proposed legislation in 1961 to

---

[3] In response to the growing prevalence of gambling and the need to determine its impact on people and places, Congress created the National Gambling Impact Study Commission ("NGISC") in 1996 to conduct a comprehensive legal and factual study of the social and economic impacts of gambling in the United States. *See* National Gambling Impact Study Commission Act, Pub. L. No. 104-169 (1996). In its final report in June 1999, the NGISC recommended, among other things, prohibiting Internet gambling "without allowing new exemptions or the expansion of existing exemptions to other jurisdictions." NGISC Final Report 5-12.

[4] NGISC Final Report 2-16.

help states enforce their gambling laws and combat organized gambling activities. The bill was passed and codified at 18 U.S.C. § 1084. Section 1084 makes it a crime for an individual engaged in the business of betting or wagering to use a "wire communication facility" to transmit in interstate or foreign commerce bets or wagers, or information assisting in the placing of bets or wagers, on any sporting event or contest. *See* 18 U.S.C. § 1084.

Because the Internet is a "wire communication facility" as defined in 18 U.S.C. § 1081, section 1084 is sufficient legal authority to prohibit the use of the Internet to engage in gambling activities related to sporting events or contests. Indeed, even in those instances where the Internet travels over non-traditional communication facilities (*e.g.*, microwave or satellite), the "wire communication facility" definition still applies, because the statutory definition includes facilities other than wire and cable that can aid in the transmission of data between "the points of origin and reception of such transmission," 18 U.S.C. § 1081.

Accordingly, law enforcement agencies are currently prosecuting individuals engaged in the business of betting or wagering in foreign countries who knowingly transmit illegal sports bets and wagers to or from U.S. residents. For example, in March 1998, the United States Attorney's Office for the Southern District of New York filed criminal complaints against 22 defendants for conspiracy under 18 U.S.C. § 371 to violate section 1084 and with section 1084 violations for the operation of online gambling sites. The websites involved in this prosecution were operated in countries in the Carribean and South America, including the Dominican Republic, Curacao, and Antigua. As of the time of this report, several defendants have pled guilty while others await trial.

Other federal statutes that may be relevant to online gambling operations include 18 U.S.C. § 1953 (interstate transportation of wagering paraphernalia); 18 U.S.C. § 1955 (prohibition of illegal gambling businesses); 18 U.S.C. §§ 3001-3007 (Interstate Horseracing Act); 18 U.S.C. §§ 1301-1307 (criminal statutes relating to lotteries); and 28 U.S.C. §§ 3701-3704 (prohibiting any lottery, sweepstakes, or other wagering scheme based directly or indirectly on one or more competitive games in which amateur or professional athletes play).

3. Investigatory Challenges

On the one hand, as noted above, existing laws have provided the basis for successful prosecutions against Internet gambling. The use of credit cards for the bulk of gambling over the Internet also means that detailed records of such transactions are likely to exist. These records may be used as evidence of criminal conduct once alleged gambling operations have been identified. Indeed, the existence of such records may well have reduced the level of illegal, online casino gambling that is conducted from U.S.-based website operators. On the other hand, however, online casino gambling has largely shifted to offshore locations, where it may be difficult for U.S. law enforcement agencies to gain access to relevant records. In addition, the use of fraudulently obtained credit card numbers can limit the usefulness of transaction records generated by the use of such cards.

Some legal changes are also needed. Although existing federal laws provide an adequate basis for prosecuting traditional forms of gambling on the Internet, new telecommunications technology has brought about entirely new types of electronic gambling, such as interactive Internet

poker and blackjack, that some gambling operations claim are not prohibited by section 1084 as it currently exists. As a result, section 1084 needs to be amended to clarify the law and to remove any doubt as to whether new types of gambling activities made possible by emerging technologies are prohibited.

The Department of Justice, working with the Departments of Commerce and Treasury and the Office of the U.S. Trade Representative, has drafted amendments that would ensure that individuals in the business of betting and wagering do not use communications facilities to transmit bets or wagers in interstate or foreign commerce, within the special maritime and territorial jurisdiction of the United States, or to or from any place outside the jurisdiction of any nation with respect to any transmission to or from the United States. Specifically, these amendments would, among other things:

> clarify that section 1084 applies to all betting or wagering (not merely betting or wagering on sports events) and includes the transmission of bets and wagers over any communication facilities;
>
> require any person, not just a common carrier, that provides a communications facility to an individual in the business of betting and wagering to cooperate with law enforcement agencies;
>
> apply section 1084 to those engaged in the business of betting or wagering who are located outside the territorial jurisdiction of the United States, when those individuals knowingly facilitate or aid in unlawful betting and wagering by transmitting a bet or wager, or information assisting in the placing of a bet or wager, to or from an individual located within the United States;
>
> clarify that section 1084 does not prohibit the lawful use of communication facilities in the operation of state lotteries; and
>
> clarify that section 1084 does not amend or repeal the Indian Gaming Regulatory Act.

Last year, both the House and the Senate introduced The Internet Gambling Prohibition Act of 1999 (H.R. 3125 and S. 692); the Senate version passed in November 1999. This proposed legislation, however, would leave traditional gambling statutes in effect for non-Internet media, while creating special rules for Internet gambling. This non-technology-neutral approach would create overlapping and inconsistent federal gambling laws. In addition, these legislative proposals contain a number of broad exemptions from its general prohibition on Internet gambling. Such exemptions are not only questionable as a matter of policy, but, because they would apply only to Internet gambling, they would exacerbate the problems created by the existence of a separate legal framework for Internet gambling.

4. Conclusions

Existing federal laws generally prohibit individuals from transmitting bets or wagers (using a "wire communication facility," which includes the Internet) on sporting events or contests in the U.S. The advances of the Internet, however, have made it necessary to update existing federal laws to ensure that they are technology-neutral and prohibit new as well as traditional forms of online gambling activities. Law enforcement also needs better mechanisms by which to track and identify online gambling businesses. The anonymous nature of the Internet complicates the ability of law enforcement to successfully track online gambling operators.

APPENDIX G – INTERNET SALE OF ALCOHOL

5. Nature of the Potentially Unlawful Conduct

Internet sales of alcohol beverages have caused direct shipments of such beverages to consumers to proliferate. Selling over the Internet allows small alcohol producers to reach consumers well beyond their immediate area. These Internet sales of alcohol beverages enable adults – and, potentially, minors – to receive products that are not ordinarily available through traditional distribution channels.

Fifteen states have established reciprocal arrangements that permit the shipment of wine (but not beer or distilled spirits) into their jurisdictions from one reciprocal state to another. Sales by alcohol marketers are not, however, limited to consumers in other reciprocal states. In many cases, these marketers may ship to consumers in other states, a practice that may violate state alcohol control laws.[1] Even if federal excise taxes are paid on these products, direct shipments to consumers across state lines causes a loss of state tax revenue and may result in federal and state regulatory violations. Such regulatory violations may include deliveries to underage persons and the sale of unregistered brands in a state. The sale of unregistered brands results in a loss of state registration fees, state excise tax revenues, and local sales tax revenues.

6. Analysis of Existing Law

Under the Federal Alcohol Administration Act, the Bureau of Alcohol, Tobacco and Firearms ("ATF") issues "basic permits" to importers, producers (except brewers), and wholesalers of alcohol beverages. *See* 27 U.S.C. § 204. Retailer sellers of alcohol beverages are not required to have a federal permit. The Webb-Kenyon Act, 27 U.S.C. § 122, prohibits the shipment of alcohol beverages into a state in violation of state law. Although the Webb-Kenyon Act has no separate penalty provisions, basic permits are conditioned on compliance with that statute.

As a result, ATF may, depending on the circumstances, take administrative action against a permittee that ships alcohol beverages into a state in violation of that state's law. ATF may also intervene if there is a continuing material adverse impact upon a state by an out-of-state permittee. Many of the entities selling on the Internet are, however, state-licensed retailers that do not hold federal basic permits and, therefore, are not subject to ATF's administrative sanctions against permittees.

Also relevant are the liquor traffic provisions of 18 U.S.C. ch. 59, which require any shipment of alcohol beverages in interstate commerce to have a bill of lading that identifies its contents, and which require deliveries to be restricted to the consignee. Some state laws allow

---

[1] *See* Alcohol Sales and the Twenty-First Amendment: Hearings Before the Senate Comm. on the Judiciary, 106th Cong., 1st Sess. (Mar. 9, 1999) (statement of John DeLuca, Wine Institute of California).

limited quantities of alcohol beverages to be shipped directly to consumers, although in some instances notifications to state alcohol agencies may be required.

3. Investigatory Challenges

The primary issue concerning the sale of alcohol beverages over the Internet is the difficulty sellers have in determining whether a purchaser is underage. Some minors could conceivably seek to use credit cards, legitimately or not, to place an order through the Internet and have alcohol beverages delivered through a shipping company. Several websites require purchasers to "certify" that they are of legal age either by clicking on part of the webpage or by faxing a copy of a driver's license. Restricting the delivery of alcohol beverage to situations where proof of age is obtained and recorded would assist in preventing access to alcohol beverages by underage persons. Currently, however, there is a significant potential for abuse in the sale of alcohol to minors.

A second investigatory issue relates to the broader issue of jurisdiction. An out-of-state seller that sells alcohol beverages through a website is not generally licensed by the state, and state courts often have difficulty establishing jurisdiction over such sellers. Under certain circumstances, as noted above, ATF may take administrative action against a permittee that ships alcohol beverages into a state in violation of the laws of that state. This authority would not reach situations where a retailer in one state ships to a purchaser in another state, because retailers are not required to have basic permits. But if the in-state purchaser resells the alcohol beverages, the out-of-state retailer then becomes a wholesale agent, against whom ATF may take enforcement action.

4. Specific Federal Legislative Initiatives

The Violent and Repeat Juvenile Offender Accountability and Rehabilitation Act of 1999 (H.R. 1501 and S. 254, 106th Congress), as passed by the Senate last year, contained two provisions related to Internet sales of alcohol beverages. Although these proposals were not ultimately passed, they are likely to be advanced again:

> The first provision, sponsored by Senators Byrd and Hatch and Representative Ehrlich, would amend the Webb-Kenyon Act, 27 U.S.C. § 122, to allow state Attorneys General to obtain preliminary and permanent injunctions in federal court against persons who engage in any act that constitutes a violation of state law regulating the importation or transportation of alcohol beverages.
>
> The second provision, sponsored by Senator Feinstein, would amend the liquor trafficking prohibitions, *see* 18 U.S.C. ch. 59, to require persons who ship alcohol beverages in interstate commerce to label the packages as containing alcohol beverages and to require shipping companies to obtain the signature of the person receiving delivery and to verify that that person is of legal age for the purchase of alcohol beverages within the receiving state.

In addition, in August 1999, the House of Representatives passed the Twenty-First Amendment Enforcement Act, H.R. 2031, which would amend the Webb-Kenyon Act to permit state Attorneys General to obtain injunctions in federal court (an approach similar to the first provision in the juvenile crime bill noted above). The bill provides that nothing in it permits state regulation or taxation of Internet services or authorizes injunctions against interactive computer services or electronic communications services.

5. Conclusions

As existing laws address the legality of shipping and selling alcohol beverages in interstate commerce, the primary issue concerning the sale of alcohol over the Internet is the potential anonymity of the buyer. The anonymous nature of the Internet makes its difficult, using current technology, for a seller to verify at the time of sale whether a prospective purchaser is of legal drinking age. In addition, the Internet facilitates direct shipments of alcohol beverages to consumers across state lines, resulting in a loss of state registration fees and state excise and local sales tax revenues and possibly resulting in federal or state regulatory violations.

APPENDIX H – ONLINE SECURITIES FRAUD

1. Nature of the Potentially Unlawful Conduct

The Internet has had a profound effect on how investors research and trade securities. Millions of investors are signing on to the Internet to obtain investment information and to execute trades. Recent estimates are that close to 16 percent of all equity trades are conducted online.[1] The number of online accounts open as of the second quarter of 1999 (nearly 10 million) is nearly triple the number open as recently as 1997.[2] The Internet has brought significant benefits to investors, including enhanced access to information (both in speed and quantity) and lower costs to execute trades.

Unfortunately, the Internet also has opened new avenues for fraud artists to attempt to swindle the investing public. This is because the Internet offers perpetrators of securities fraud a medium to commit their crimes that is speedy, cheap, easy to use, and relatively anonymous. For the most part, there are three categories of securities frauds that have been encountered online by law enforcement.

> *Market Manipulation* – This category of fraud most often involves attempts to artificially inflate a stock's price by creating demand for thinly traded lower-priced securities. The manipulators create the demand through the dissemination of false and misleading information, such as phony announcements pertaining to strategic alliances, future earnings, mergers, or other important corporate developments. The Internet has proven to be fertile ground for such manipulations, because information can be disseminated with the simple click of a mouse to millions of users via websites, newsletters, spam, message boards, and other Internet media. The manipulator normally owns shares in the company's stock and sells during the run-up that the manipulator creates. This fraud is commonly known as a "pump-and-dump" scheme. The PairGain case discussed at the beginning of this report is an example of a market manipulation case.
>
> *Offering Frauds* – These cases generally involve either false or misleading offerings of securities. Falling into this category of cases are pyramid and Ponzi schemes, and affinity frauds targeted at specific racial, ethnic, or religious groups. In addition, there have been numerous fraudulent offerings of non-traditional securities over the Internet, such as offerings for "prime bank" programs and other esoteric securities, including interests in eel farms, coconut plantations, and fictional countries. Persons offering these securities

---

[1] *See* Report of SEC Commissioner Laura S. Unger, Online Brokerage: Keeping Apace of Cyberspace 1 (Nov. 1999).

[2] *See id.*

often violate the law by failing to register as broker-dealers. The SEC has successfully tracked many of these offerings and conducted a May 1998 "sweep," in which it charged 26 individuals and companies for engaging in bogus securities offerings on the Internet.

Illegal Touting – This type of securities fraud takes place when persons are paid to hype a company's stock without making legally required disclosure of the nature, source, and amount of their compensation. This disclosure is necessary because investors have a right to know whether information they are receiving is objective or "bought and paid for." The SEC has brought two Internet touting "sweeps" charging a total of 57 individuals and companies.

These three categories are not exhaustive. There are other securities law violations taking place on the Internet, including unregistered offerings of securities as well as broker-dealer registration violations. For example, in July 1999, the SEC coordinated the filing of four so-called "free stock" actions charging those who offered securities over the Internet with having failed to register those offerings. Two of those actions also alleged fraud.

2. Analysis of Existing Law

The existing statutory framework provided by the federal securities laws has generally been adequate in the federal government's efforts to fight online securities fraud. As with the other examples of Internet-facilitated unlawful conduct discussed in this report, however, as our experience fighting such conduct continues to evolve, it may be necessary to revisit whether any new legislation or rule-making is needed.

Section 10(b) of the Securities Exchange Act of 1934, 15 U.S.C. § 78j(b), and Rule 10b-5 thereunder, 17 C.F.R. § 240.10b-5, are the primary authorities used by the SEC to combat market manipulation and other frauds in the securities market. These provisions make it unlawful to use a fraudulent scheme or to make material misrepresentations and omissions in connection with the purchase or sale of any security. Both section 10(b) and Rule 10b-5 were drafted broadly to capture new and unforeseen frauds.[3] Most of the cases brought by the SEC have charged defendants with violating section 10(b).

Unlawful touting is covered by section 17(b) of the Securities Act of 1933, 15 U.S.C. § 77q(b), which makes it unlawful to use interstate facilities to fraudulently offer or sell securities. Specifically, this statute deems it unlawful for any person to give publicity to, or otherwise tout, a security in exchange for compensation without full disclosure of the fee arrangement. It applies to information spread in cyberspace just as it does to information spread by newsletters, radio, or any other traditional media.

---

[3] *See, e.g.,* Affiliated Ute Citizens v. United States, 406 U.S. 128, 151 (1972) ("The[] proscriptions [of section 10(b) and Rule 10b-5] are broad and . . . obviously meant to be inclusive").

Individuals engaged in unregistered offerings of securities on the Internet may be liable under section 5 of the Securities Act, 15 U.S.C. § 78e, unless the offering qualifies for one of certain exemptions. This law is designed to assure that investors have adequate information upon which to base their investment decisions. The SEC has brought several cases charging violations of this statute in connection with Internet offerings, including four cases brought in July 1999 against issuers of so-called "free" stock. The SEC has also brought cases charging unlawful offerings of securities on an Internet auction site.

The federal securities laws also impose registration requirements upon anyone acting as a broker or dealer and upon large investment advisers.[4] Those persons acting in these capacities by virtue of conduct on the Internet are required to register with the SEC to the same extent as those acting in the offline world are.

3. Specific Federal Initiatives

The SEC has devoted substantial resources to policing the Internet, including creating the Office of Internet Enforcement ("OIE") in July 1998. OIE, currently staffed with ten attorneys, regularly conducts investigations on the Internet, referring matters to other SEC staff, as well as to other agencies and the self-regulatory organizations, when appropriate. OIE also conducts national law enforcement training. For example, in November 1999, OIE hosted the first-ever Internet securities fraud training program, attended by more than 300 law enforcement personnel nationwide. OIE also oversees the Commission's "cyber-force," a group of approximately 240 SEC staff members who use the Internet as part of their investigations.

As a result of these and other efforts, the SEC has brought approximately 110 Internet-related enforcement actions since 1995, with the vast majority coming in the past two years as the use of the Internet by prospective investors has surged. The SEC has articulated a 5-pronged approach to counteracting Internet fraud: (a) vigilant and flexible surveillance; (b) aggressive prosecution; (c) coordinated liaison work with other agencies, criminal prosecutors, and self-regulatory organizations; (d) investor education; and (e) the fostering of self-policing and encouraging members of the public to provide the agency with tips and complaints.

4. Investigatory Challenges

The shift of securities fraud from traditional media, such as "boiler room" telephone banks, to the Internet certainly poses new challenges for regulators. The SEC's greatest challenge to date has been one of resources. As the SEC's Director of Enforcement stated in testimony before the Senate Permanent Subcommittee on Investigations in March 1999, "Our greatest problem will likely be one of resources, as the size of our staff has remained relatively constant while the Internet has

[4] Under the National Securities Markets Improvement Act of 1996, advisers managing assets of $25 million or more generally must register with the SEC; smaller advisers register with the states. *See* 15 U.S.C. §§ 77z-3, 78mm, 80b-3a.

grown by leaps and bounds." The vastness of the Internet requires significant resources for appropriate surveillance coupled with timely investigation and prosecution of violations.

The resource issue is particularly acute with respect to the investigation and prosecution of illegal conduct. Experience shows that securities fraud artists operating on the Internet typically do not hide; rather, they operate in plain view in an attempt to reach as many potential investors as possible. The Internet offers investigators in the SEC an important window through which to observe developing frauds, and, in certain cases, to halt them before they reach investors' pockets. For example, in several of the actions comprising the SEC's May 1999 fraudulent offering sweep, the SEC stopped the fraud *before* investors lost a penny.

The Internet also poses the challenge of requiring the SEC to stay abreast of new variants of fraud and manipulation. Fraud artists often design new forms of fraud to exploit opportunities offered by the Internet. For example, the SEC's Division of Enforcement is investigating a number of websites that offer daily or periodic stock recommendations designed to generate trading momentum and an accompanying rise in the price of the underlying security. Those involved in such activities then profit by selling the security at the artificially inflated price.

An additional challenge posed by the Internet is the ability to investigate, in a timely manner, fraud artists who operate without regard to territorial borders. An individual virtually anywhere in the world, for example, can target U.S. investors without stepping foot in this country. Sophisticated scam artists also seem to think that they have a better chance of escaping detection, hiding funds, or dodging regulators if they shift operations and funds from one country to another. Accordingly, we need to ensure that our foreign counterparts also have the technical expertise needed to track Internet fraud artists. To that end, the SEC recently hosted an international symposium focused on Internet securities fraud, so that international regulatory authorities might share investigative techniques, enhance communication, and increasingly cooperate in combating cross-border securities fraud.

5. Conclusions

The federal securities law provide flexible but extensive mechanisms by which securities offenses can be prosecuted. Although the substantive laws may be adequate, law enforcement agencies still need adequate resources to counter online securities fraud. As with other types of unlawful conduct on the Internet, the interstate and foreign nature of the Internet hinders the ability of law enforcement to investigate and prosecute online criminals.

APPENDIX I – SOFTWARE PIRACY AND INTELLECTUAL PROPERTY THEFT

1. Nature of the Potentially Unlawful Conduct

The advent of powerful and inexpensive computing is bringing many changes to the way that copyrighted works are being illegally distributed, and hence to the methods that law enforcement uses to combat copyright piracy. Traditionally, copyrighted works (such as books, records, and audiotapes) and counterfeit trademarked goods have been illegally reproduced here or abroad in a factory. The copyrighted works or counterfeit goods are sold to wholesalers, and then to retailers, who in turn sell them on the street. In this type of distribution scheme, the damage to copyright owners or trademark holders, while substantial, is subject to certain technological limits. That is because the equipment necessary to reproduce the works or goods in bulk is relatively expensive, and because second-generation products (*i.e.*, copies of copies) are either impossible for the customer to make (for records and compact discs) or suffer in quality (for audio and video cassettes).

Another feature of this model of distribution is that the sale of the copyrighted works or counterfeit trademarked goods on the street is highly visible, making it likely to attract the attention of law enforcement. Once the crime problem is targeted, the nature of the distribution scheme permits law enforcement to infiltrate the organization by obtaining the cooperation of the retailer to make a case against the wholesaler, and then use the cooperation of the wholesaler to make a case against the factory owner. By this process, an entire distribution scheme can be shut down, resulting in the seizure of a substantial number of illegally copied works or counterfeit trademarked goods.

This illegal distribution of copyrighted works in the offline world continues to present a pressing problem for copyright owners, particularly for producers of books, movies, music, and computer software. Accordingly, law enforcement continues to focus attention on investigating and prosecuting offline copyright pirates. To an ever-increasing extent, however, copyright piracy is being carried out through computers. Anything capable of being digitized – that is, reduced to a series of zeros and ones – is capable of being transmitted easily from one computer to another. Pirates have used this capability of the computer to steal vast amounts of copyrighted material and to transfer it illegally to others. Similarly, counterfeit goods may be offered for sale over the Internet as legitimate goods bearing well-known trademarks. In such instances, not only is the purchaser defrauded, but the trademark holder can suffer reputational damage and lost sales opportunities.

So far, computer software companies appear to have suffered the most at the hands of these new intellectual property pirates. For example, although it is difficult to estimate the magnitude of software piracy, the Business Software Alliance ("BSA") estimates that software piracy cost the U.S. some 109,000 jobs and $991 million in tax revenue in 1998. The BSA further estimates that approximately 2 million web pages offer, link to, or otherwise reference "warez," the Internet code word for pirated software. This figure is twice the number of websites that offered pirated software a year ago, and a 20-fold increase over the past three years.

As technology increasingly permits different types of works to be easily digitized and copied, other industries are also being affected. For example, the music industry is now beginning to suffer serious losses from computer pirates. The Recording Industry Association of America estimates that

music piracy caused a loss of income in 1998 of over $300 million annually to the U.S. economy. Digital transfers of music, generally through MP3 formatted sound recordings,[1] are the most prevalent form of music piracy on the Internet. Through the Internet, cyberpirates can trade or sell individual songs or full-length albums in minutes. And within a few years, the movie industry may well also find its products routinely vulnerable to computer theft.

Moreover, the ease with which copyrighted works can be distributed is alarming. Just a few years ago, most pirated materials were distributed through Bulletin Board Services ("BBSs"), which operated like private clubs, requiring a password to gain access to the illegally copied software. Although these BBSs were a significant problem, they caused only a finite amount of harm, because access to the public was restricted. Today, the primary source of pirated computer software are websites that offer anywhere between a few to a few hundred copyrighted programs for free to anyone able to maneuver a mouse. Now, even an unsophisticated computer user can use a standard search engine, search for "warez," and find thousands of websites that offer copyrighted software for free. Even a run-of-the-mill warez site can generate hundreds or even thousands of downloads every day, with no limit to the number of additional times a downloader can transfer the same program to other users.

The proliferation of Internet piracy exposes the consumer to an increased risk of computer viruses and fraudulent software sales, weakens the software industry's ability to generate economic growth, and facilitates a host of other criminal activities. Specifically, such conduct has the following effects:

> *Consumer fraud* – Internet pirates are extending their reach to ordinary consumers who shop the Internet to find discounted, but legitimate, software. Employing a variety of schemes, including e-mail solicitations, auction sites, and seemingly legitimate software sites, these pirates hope to dupe unsuspecting consumers into purchasing pirated software (just as they do in the physical world). Individuals, as well as corporate, government and educational entities, have been victimized by fraudulent software sales through the Internet.
>
> *Economic losses* – Internet piracy and other forms of software theft also represent a substantial drain on the U.S. economy. Although some (and perhaps much) of the creative material that is allegedly pirated would never have been purchased in the first instance, some proportion of lost sales can clearly be attributed to such theft.

---

[1] MP3 is a shorthand term for MPEG-1 Layer 3, a compression algorithm adopted by the Motion Picture Experts Group. MP3, the most advanced version of the MPEG format first created in 1992, is widely available and allows users to download audio files more rapidly and to store them with less computer storage space than previously possible.

Other criminal activities – Increasingly, pirated software sales through the Internet are used to facilitate and finance other criminal activities. Many "warez" software sites generate revenue by advertising other illegal goods, services and information. The Internet is also becoming a popular marketing tool for organized crime syndicates that dominate the software counterfeiting industry. These crime syndicates use online sales of counterfeit software to fund, and launder money from, a host of other criminal activities, including drug trafficking, illegal weapons, gambling, and prostitution.

2. Analysis of Existing Law

In December 1997, Congress passed the No Electronic Theft ("NET") Act, making it a criminal offense to distribute or to reproduce copies of copyrighted works, if not authorized to do so, regardless of whether the distributor was trying to profit from the activity. The legislation was intended to fill a gap in the criminal copyright statute, highlighted in the dismissal of an indictment in United States v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994).

In *LaMacchia*, an MIT student operated a BBS over the Internet that allowed anyone with a computer and modem to send to the BBS or acquire from the BBS copyrighted software programs. His actions caused an estimated loss to copyright holders of over $1 million during the 6-week period the system was in operation. The student could not be charged with violation of the criminal law protecting copyright, 17 U.S.C. § 506, because he was not acting "for commercial purpose or private financial gain," an element of the criminal copyright offense. Instead, he was charged with conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1343. The district court dismissed the indictment, finding copyright law to be the exclusive remedy for protecting intellectual property rights from this kind of theft, even while recognizing that the existing copyright law failed to cover this conduct. The district court invited Congress to remedy this gap in the law, andCongress did so in the NET Act.

The NET Act creates a new criminal offense to cover the unauthorized distribution or reproduction of copies of copyrighted works, regardless of whether the distributor intends to profit from the activity. *See* 17 U.S.C. § 506(a)(2); 18 U.S.C. § 2319(b)(2). It establishes a felony, punishable by up to three years imprisonment, for reproducing or distributing, during any 180-day period, ten or more copies of one or more copyrighted works that have a total retail value of more than $2,500. The NET Act also:

Increases penalties for second or subsequent felony criminal copyright offenses;

Extends the statute of limitations from three to five years, bringing it in line with most other criminal statutes;

Clarifies "financial gain" to include the receipt of anything of value, including the receipt of other copyrighted works, to cover pirate operations that involve barter rather than cash transactions;

> Clarifies "reproduction or distribution" to include electronic as well as tangible means;
>
> Extends victims' rights to allow the producers of pirated works to provide a victim impact statement to the sentencing court; and
>
> Directs the U.S. Sentencing Commission to amend the Sentencing Guideline for copyright and trademark infringement to allow courts to impose sentence based on the retail value of the good infringed upon, rather than the often lower value of the infringing good.[2]

Other relevant criminal intellectual property laws include 18 U.S.C. § 2319A (bootlegging of music); 18 U.S.C. § 2320 (trademark counterfeiting); and 18 U.S.C. § 2318 (counterfeit labeling for copied items).

In October 1998, the President signed into law the Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (codified in scattered sections of 17 U.S.C.), which creates criminal penalties for circumventing a copyright protection system and prohibits the manufacture, import, sale, or distribution of devices or services used for such circumvention. The statute exempts circumvention for security testing or encryption research. The statute also protects Internet and online service providers from being held liable for copyright infringements made by their customers.

Another important law is the Economic Esponiage Act ("EEA"), 18 U.S.C. § 1831 *et seq.*, which provides federal penalties for the theft of trade secrets. Trade secrets are an integral part of virtually every aspect of trade, commerce, and business, and the security of trade secrets is essential to maintaining the health and competitiveness of critical segments of the U.S. economy. In 1994, the FBI established an economic counterintelligence program as part of its national security strategy. The EEA, passed in 1996, complemented that effort by filling several gaps in the law and by creating two new felonies. Section 1831 punishes any person or company that steals trade secrets on behalf of a foreign government or entity. *See* 18 U.S.C. § 1831(a). Persons convicted under this provision face up to 15 years imprisonment and up to $500,000 in fines. *See id.* Fines for organizations convicted under this law can range up to $10 million. *See* § 1831(b). Section 1832 punishes the theft of trade secrets for mere economic benefit and does not require intent to benefit a foreign entity.

---

[2] The current Sentencing Guideline for copyright and trademark violations, § 2B5.3, requires courts to calculate the applicable sentence based on the retail value of the *infringing* items. For years, this focus on the low retail value of the infringing goods, without regard to the actual value of the legitimate goods, has led courts to impose lower sentences on defendants who commit intellectual property crimes than those who commit other similar crimes. As a result of these lower sentences, law enforcement agencies and prosecutors may be reluctant to commit scarce resources to investigating and prosecuting these cases. The lack of enforcement, in turn, contributes to the perception that intellectual property crimes are associated with high profits and low risks, which in turn helps fuel the growth of these crimes.

See id. § 1832(a). It carries a maximum 10-year jail term and up to $500,000 in fines for individuals and $5 million for organizations. *See* § 1832(a) & (b).

The EEA defines a trade secret broadly to include any proprietary information that is reasonably protected from public disclosure and that derives independent economic value for the rightful possessor from being a secret. *See* 18 U.S.C. § 1839(3). Importantly, the EEA protects the victim's trade secret from public disclosure throughout the entire court process. *See* § 1835.

3. Specific Federal Initiatives

The Department of Justice (including the FBI) and the Customs Service have responded to the theft of intellectual property facilitated by the Internet by placing increased emphasis on investigating and prosecuting such crimes. Last year, these agencies announced the establishment of a law enforcement initiative aimed at combating the growing challenge of piracy and counterfeiting of intellectual property, both domestically and internationally. The initiative initially targets the New York-New Jersey metropolitan area, South Florida, the Boston metropolitan area, and the high-tech corridors of California. Internationally, the initiative pledges support from the Department of Justice, including the FBI, for existing efforts of the State Department, the Customs Service, and trade agencies with specialized expertise in intellectual property issues (the Office of the U.S. Trade Representative, the Department of Commerce's Patent & Trademark Office, and the Copyright Office) to enhance their technical assistance capabilities and training priorities. The initiative also pledges law enforcement support of interagency efforts intended to help U.S. trading partners strengthen and enforce intellectual property laws.

The Department of Justice's Computer Crime and Intellectual Property Section ("CCIPS"), created within the Criminal Division in 1996, leads the Department of Justice's efforts to combat intellectual property crime on the Internet. As its name indicates, CCIPS is responsible for coordinating the Department's policies regarding computer crime and the enforcement of criminal laws protecting intellectual property. The Section has particular expertise in the area of computer-based copyright theft. For instance, CCIPS published a 175-page manual entitled *Federal Prosecution of Violations of Intellectual Property Rights: Copyrights, Trademarks and Trade Secrets*. This manual has been provided to each of the 93 U.S. Attorney's Offices and is available online at www.usdoj.gov/criminal/cybercrime. It provides agents and prosecutors with a detailed resource for undertaking prosecutions in this area of the law. In addition, CCIPS works closely with computer and telecommunications coordinators ("CTC") in each U.S. Attorney's Office. CTCs are prosecutors who are specially designated by each U.S. Attorney to be resident experts in that district on high-tech crime and who have specialized training in both computer crime and intellectual property protection.

CCIPS also provides training to state and local agents and prosecutors in a variety of settings and is active in training law enforcement officials from other nations. Section attorneys have traveled to Russia, Egypt, and many other countries to give guidance to our counterparts there, and regularly instruct foreign officials visiting the United States on U.S. laws and techniques for combating copyright piracy. These efforts are particularly important to the United States, because

many of the products being illegally copied abroad are produced by U.S. companies, and because computers make it easy to send such pirated works across international boundaries.

In September 1999, President Clinton signed an appropriations bill that included a provision that created the National Intellectual Property Law Enforcement Coordination Council. The Council is chaired by the Commissioner of Patents and Trademarks and the Assistant Attorney General for the Criminal Division of the Department of Justice. Other members of the Council include the Under Secretary of State for Economic, Business, and Agricultural Affairs; the Deputy United States Trade Representative; the Commissioner of Customs; and the Under Secretary of Commerce for International Trade. The Council's mission is to coordinate domestic and international intellectual property law enforcement matters among federal and foreign entities. It is required to report annually on its coordination activities to the President and to the Appropriations and Judiciary Committees of the Senate and the House of Representatives.

In addition, in October 1999, Customs Commissioner Kelly announced the opening of the National Intellectual Property Center, a multi-agency center based at Customs headquarters in Washington, D.C. Investigators from Customs and the FBI provide the core staffing for the Center, which will focus on coordinating the investigation of software piracy and other domestic intellectual property offenses.

The Customs Service's CyberSmuggling Center is working closely with industry representatives and is currently investigating distributors in Russia, Singapore, Malaysia, and the United Kingdom of commercial quantities of pirated U.S. merchandise (such as business software, video games, motion picture movies, and sound recordings) to customers worldwide over the Internet. The pirated merchandise can be ordered from the distributors via Internet mail order or through direct digital download, which allows large volumes of merchandise to be distributed to a worldwide audience in minutes.

The CyberSmuggling Center is also investigating distributors in the U.S. who appear to be involved in importing and distributing commercial quantities of traditional counterfeit U.S. merchandise, such as watches, sunglasses, and handbags, via the Internet. The Center recently initiated an enforcement operation that targeted over 30 such online distributors.

4. Investigatory Challenges

Pursuing copyright pirates who operate in cyberspace presents new challenges for copyright owners and for law enforcement agencies. First, unlike the equipment necessary to make large quantities of physical copies of tapes and discs, computers that can easily copy digital information are relatively inexpensive. Second, with digital copies, there is no deterioration in quality when second or third generation copies are made. Accordingly, a copyrighted work can be placed on a website and copied by hundreds of people. Those people can then redistribute the copy to others, illegally spreading the material around the world within minutes.

For law enforcement, electronic copyright violations may easily escape detection, because, rather than taking place openly in physical space, they take place hidden in cyberspace. Before the

advent of inexpensive electronic distribution, international traffickers of pirated copyrighted material had to bring that material physically into or out of the country, giving law enforcement authorities at least an opportunity to seize it. Now, of course, such materials can enter the United States electronically without passing through any border or physical location that is subject to government monitoring or inspection. As such, locating and identifying online copyright pirates can be difficult. Even when law enforcement agents focus on particular computer copyright violations, the lack of a hierarchical distribution scheme makes it difficult for a single case to make a noticeable impact on the amount of copyrighted material available through illegal channels: the software no longer available from one website can simply be found elsewhere.

Finally, it is important to note that while the offline distribution of copyrighted works can be investigated by any law enforcement agent, computer violations require technically adept agents. These agents are in short supply, despite the efforts of federdal law enforcement agencies to hire and train agents to deal with computer crime. Even when investigative agencies have such resources, they are often needed to investigate other computer crimes, such as attacks on the confidentiality, integrity, and availability of computer systems and data.

5. Conclusions

Generally, the substantive federal laws governing theft of intellectual property on the Internet are adequate. The ease with which offenders can duplicate and distribute protected works on the Internet, however, has raised investigatory challenges for law enforcement. To address these challenges, there need to be, among other things, improved technologies to find the distributors, investigators trained to use those tools, and effective international agreements to bring the offenders to justice. In addition, the current Sentencing Guidelines pertaining to intellectual property offenses do not provide adequate sentences and have resulted in law enforcement agencies and prosecutors being reluctant to commit scarce resources to investigating and prosecuting criminal intellectual property cases.

APPENDIX J – MULTILATERAL EFFORTS

1. Council of Europe ("COE")

The COE is an international organization based in Strasbourg, France which was established by ten Western European countries in the wake of World War II. Today, it has a pan-European membership of 41 countries, including the Baltic states, Russia, and Turkey. Its primary mission is to strengthen democracy, human rights, and the rule of law throughout its member states. In 1989 and 1995, the COE adopted recommendations on computer-related crime that called on member states to consider computer crimes when either reviewing or proposing domestic legislation. These recommendations also contained principles on such topics as search and seizure, technical surveillance, electronic evidence, encryption, and international cooperation.

In February 1997, a Committee of Experts on Crime in Cyberspace was formed to examine computer crime and related problems in criminal procedure law. Representatives from the United States were invited to attend as non-voting observers. The Committee intends to draft a "Cybercrime Convention" that will define cybercrime offenses and will address such topics as jurisdiction, international cooperation, and search and seizure. The Committee plans to have a draft Convention completed by December 2000. After approval by the Committee of Ministers, the Convention will be open for signature by COE members and by non-member states that participated in its drafting. (If the United States were to become a signatory to the Convention, the U.S. Senate would have to ratify the Convention, as with any international treaty.)

2. Group of Eight ("G-8")

The G-8 leading industrialized nations is comprised of the United States, the United Kingdom, France, Germany, Italy, Canada, Japan, and Russia. The group was formed in 1975 at an Economic Summit in France, and since then, its agenda has expanded to include many topics. The G-8 has a "summit-based" process, which means that the heads of state of each member country meet annually. At their 1996 Summit in Paris, the heads of state adopted 40 recommendations to fight international crime, with high-tech and computer-related crime among the topics specifically addressed.

To implement these recommendations and to enhance the abilities of law enforcement in combating high-tech and computer-related crime, a G-8 Subgroup on High-tech Crime was formed in January 1997. As of February 2000, the Subgroup on High-tech Crime has met 17 times. The Subgroup has: (1) established a 24-hour/7-day-a-week ("24/7") network of high-tech points of contact for law enforcement in each of the G-8 countries and in a number of non-G-8 countries (with efforts underway to continue to expand the network); (2) hosted an international computer crime training conference in November 1998 for G-8 law enforcement officials; (3) reviewed G-8 legal systems as they concern high-tech crime, and related work to fill existing gaps; and (4) worked on enhancing G-8 abilities to locate and identify criminals who use networked communications (*e.g.*, preservation of and access to historical traffic data and future ("real-time") traffic data).

These efforts are having concrete results. The 24/7 point-of-contact network has resulted in the preservation of perishable electronic evidence across borders quickly enough to catch cybercriminals and to prevent crime. The U.S. now receives or makes several requests a month through the 24/7 network for electronic evidence in cases as far-ranging as extortion and bomb-threats, murder, fraud, and computer crime.

A cornerstone of the G-8's work on high-tech crime has been consultation and cooperation with industry. Representatives from hardware manufacturers, telecommunications carriers, and ISPs have made presentations at Subgroup meetings and have discussed concrete steps law enforcement and industry can take together to accelerate cooperation between the two. The Subgroup's ongoing work with industry includes: adopting a process that allows the companies that are developing technical standards, including next-generation Internet technologies, to take into account public safety needs; consulting within governments to ensure that new data protection policies do not provide havens for criminals; standardizing law enforcement requests for assistance to industry, to allow industry to respond more quickly and with less expense; and developing 24-hour points-of-contact with critical ISPs. The Subgroup is also planning a G-8 industry conference on high-tech crime that would bring together high-tech crime-fighters and private sector representatives from the G-8 countries.

3. Organization for Economic Co-Operation and Development ("OECD")

The OECD, housed in Paris, France, is an intergovernmental forum of 29 countries with market-based economies, including the United States. It seeks to promote economic growth, trade, and development. Representatives from the FTC and the Department of Commerce have been working actively with the OECD's Consumer Policy Committee to develop Guidelines for Consumer Protection in the Context of Electronic Commerce ("Guidelines"). The Guidelines were formally adopted by the OECD Council in December 1999.

The Guidelines, though not legally binding, reflect an international consensus among member countries as they begin to formulate and implement consumer protections for e-commerce; as the private sector begins to develop self-regulatory schemes; and as consumers begin to form expectations of fair online business practices. The overarching principle in the Guidelines is that consumers should be afforded effective and transparent protection in e-commerce that is not less than the protection afforded in other forms of commerce. The Guidelines also call for fair business, advertising, and marketing practices; disclosure of information sufficient to allow consumers to make informed choices; clear processes for confirming transactions; secure payment mechanisms; and timely and affordable dispute resolution and redress processes.

The Guidelines benefitted from a participatory drafting process, which actively sought input from consumers, industry, and academia. Positions taken by the U.S. during the drafting process were informed by public submissions and dialogue in connection with a June 1999 FTC workshop on "U.S. Perspectives on Consumer Protection in the Global Economic Marketplace."

4. International Marketing Supervision Network ("IMSN")

The IMSN is a membership organization that consists of the consumer protection law enforcement authorities of over two dozen countries. The FTC represents the IMSN for the U.S. The mandate of the IMSN is to share information about cross-border commercial activities that may affect consumer interests and to encourage international cooperation among law enforcement agencies. The U.S. has led the development of the organization's website (www.imsnricc.org), which features both a members-only site as well as a public site.

Under the auspices of the IMSN, the U.S. has developed on-going cooperative relationships with consumer protection law enforcement agencies around the world. These relationships have yielded tangible results for U.S. consumers. For example, in 1997, the FTC targeted an Internet domain name scam being operated out of Australia and alerted its IMSN counterpart, the Australian Competition and Consumer Commission ("ACCC"). The ACCC brought an action against the company and its principal in federal court in Australia for misleading and deceptive conduct. The case was settled in June 1999 by the ACCC with the establishment of a trust fund, which will return $A 250,000 to victims worldwide, including almost 900 U.S. consumers. Similarly, in 1999, the ACCC and another IMSN counterpart, the Portugese Instituto do Consumidor, provided the FTC valuable assistance with a case involving an Internet scam that cloned everyday websites and used the copy-cat sites to barrage unsuspecting consumers with pornographic material.

5. Cross-Border Fraud Task Forces

In addition to working with formal multilateral international organizations, U.S. consumer protection law enforcement agencies combat cross-border Internet fraud through less formal arrangements, such as task forces. For example, the U.S.-Canada Telemarketing Fraud Task Force and the Mexico-U.S.-Canada Health Care Fraud Task Force provide a framework for cooperation, information-sharing, and joint educational efforts in the areas of telemarketing fraud and health care fraud, respectively. Similar task forces could be useful in facilitating cooperation on Internet-related matters.