



# 1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY

---

**Cyberstalking:  
A New Challenge for Law Enforcement and Industry**  
**A Report from the Attorney General to the Vice President**  
**August 1999**

---

## Introduction

The new millennium is fast approaching, and the information superhighway is undergoing rapid growth. The Internet and other telecommunications technologies are promoting advances in virtually every aspect of society and every corner of the globe: fostering commerce, improving education and health care, promoting participatory democracy in the United States and abroad, and facilitating communications among family and friends, whether across the street or around the world. Unfortunately, many of the attributes of this technology - low cost, ease of use, and anonymous nature, among others - make it an attractive medium for fraudulent scams, child sexual exploitation, and increasingly, a new concern known as "cyberstalking."

*"Make no mistake: this kind of harassment can be as frightening  
and as real as being followed and watched in your neighborhood or  
in your home."*

Vice President Al Gore

Recognizing this emerging problem, Vice President Al Gore asked the Attorney General on February 26, 1999, to study the problem and to report back with recommendations on how to protect people from this threat. Responding to this request, this report explores the nature and extent of cyberstalking; surveys the steps law enforcement, industry, victims groups, and others currently are taking to address the problem; analyzes the adequacy of current federal and state laws; and provides recommendations on how to improve efforts to combat this growing problem.

As discussed below, the nature and extent of the cyberstalking problem is difficult to quantify. In addition, while some law enforcement agencies are responding aggressively, others are not fully aware of the problem and lack the expertise and resources to pursue cyberstalking cases. Similarly, while some Internet Service Providers (ISPs) have taken affirmative steps to crack

down on cyberstalking, others have not, and there is a great deal more that industry can and should do to empower individuals to protect themselves against cyberstalking and other online threats.

Indeed, current trends and evidence suggest that cyberstalking is a serious problem that will grow in scope and complexity as more people take advantage of the Internet and other telecommunications technologies. The analysis and recommendations contained in this report offer a framework for an initial response to the problem. These recommendations, however, are only a first step. Important advances can be made if industry, law enforcement, victims service providers and support groups, and others work together to develop a more comprehensive and effective response to this problem. Ultimately, however, the first line of defense will involve industry efforts that educate and empower individuals to protect themselves against cyberstalking and other online threats, along with prompt reporting to law enforcement agencies trained and equipped to respond to cyberstalking incidents.

### **What Is Cyberstalking?**

Although there is no universally accepted definition of cyberstalking, the term is used in this report to refer to the use of the Internet, e-mail, or other electronic communications devices to stalk another person. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim's immediate family; and still others require only that the alleged stalker's course of conduct constitute an implied threat.<sup>(1)</sup> While some conduct involving annoying or menacing behavior might fall short of illegal stalking, such behavior may be a prelude to stalking and violence and should be treated seriously.

### Protecting Children from On-Line Dangers

Although the Internet and other forms of electronic communication offer new and exciting opportunities for children, they also expose children to new threats. For example, Federal law enforcement agencies have encountered numerous instances in which adult pedophiles have made contact with minors through online chat rooms, established a relationship with the child, and later made contact for the purpose of engaging in criminal sexual activities.

Federal, state, and local law enforcement agencies have responded aggressively to protect children from online sexual predators. For example, in 1995, the Federal Bureau of Investigation launched an undercover initiative, dubbed Innocent Images, to combat the exploitation of children via commercial online services. Based in Calverton, Maryland, "Innocent Images" is the central operation and case management system for all FBI undercover online child pornography and child sexual exploitation investigations. As of December 31, 1998, the initiative has resulted in 232 convictions. Similarly, the U.S. Customs Service's CyberSmuggling Center, based in Sterling, Virginia, plays an important role in combating sexual exploitation of children via the Internet and other online communications media. The Center develops leads and tips for law enforcement investigation, receives complaints via the U.S. Customs Service website, and coordinates undercover operations against international child pornography and child sexual exploitation rings. The National Center for Missing and Exploited Children unveiled a new CyberTipline in March 1998 to serve as a national online clearinghouse for tips and leads about child sexual exploitation. ([www.cybertipline.com](http://www.cybertipline.com))

The Department of Justice, through the Office of Juvenile Justice and Delinquency Prevention's Missing and Exploited Children Program (MECP), provides funding to state and local law enforcement agencies to create multijurisdictional responses to prevent and combat Internet crimes against children. In 1998, ten state and local agencies received grants under MECP; an additional eight task forces will be funded in 1999.

There are steps parents and others can take to protect children from online dangers. Parents should teach their children to follow the common-sense "rules of the road" for the Internet, including the need to protect their privacy in the online world. The FBI, for example, has prepared an online "Parent's Guide to Internet Safety." ([www.fbi.gov](http://www.fbi.gov)) Moreover, individuals should report inappropriate behavior to their Internet Service Provider (ISP) or, if it involves potentially illegal conduct, to appropriate law enforcement agencies. Law enforcement agencies need to establish and/or improve programs that train their personnel to recognize the seriousness of online child sexual exploitation and how to investigate this new form of criminal conduct. They also need to work closely with ISPs and others to facilitate communication and cooperation. Finally, private companies, including ISPs, need to provide parents and children with effective tools to protect children from online exploitation, including filtering technology, parental controls, and other efforts. ISPs also need to establish clear policies that prohibit online solicitation or exploitation of children and to take appropriate action when such incidents come to their attention, as is now required under federal law. See U.S.C. 13032.

### Nature and Extent of Cyberstalking

#### *An existing problem aggravated by new technology*

Although online harassment and threats can take many forms, cyberstalking shares important characteristics with offline stalking. Many stalkers - online or off - are motivated by a desire to exert control over their victims and engage in similar types of behavior to accomplish this end.

As with offline stalking, the available evidence (which is largely anecdotal) suggests that the majority of cyberstalkers are men and the majority of their victims are women, although there have been reported cases of women cyberstalking men and of same-sex cyberstalking. In many cases, the cyberstalker and the victim had a prior relationship, and the cyberstalking begins when the victim attempts to break off the relationship. However, there also have been many instances of cyberstalking by strangers. Given the enormous amount of personal information available through the Internet, a cyberstalker can easily locate private information about a potential victim with a few mouse clicks or key strokes.

The fact that cyberstalking does not involve physical contact may create the misperception that it is more benign than physical stalking. This is not necessarily true. As the Internet becomes an ever more integral part of our personal and professional lives, stalkers can take advantage of the ease of communications as well as increased access to personal information. In addition, the ease of use and non-confrontational, impersonal, and sometimes anonymous nature of Internet communications may remove disincentives to cyberstalking. Put another way, whereas a potential stalker may be unwilling or unable to confront a victim in person or on the telephone, he or she may have little hesitation sending harassing or threatening electronic communications to a victim. Finally, as with physical stalking, online harassment and threats may be a prelude to more serious behavior, including physical violence.

#### Offline vs. Online Stalking -- A Comparison<sup>(2)</sup>

##### Major Similarities

Majority of cases involve stalking by former intimates, although stranger stalking occurs in the real world and in cyberspace.

Most victims are women; most stalkers are men.

Stalkers are generally motivated by the desire to control the victim.

##### Major Differences

Offline stalking generally requires the perpetrator and the victim to be located in the same geographic area; cyberstalkers may be located across the street or across the country.

Electronic communications technologies make it much easier for a cyberstalker to encourage third parties to harass and/or threaten a victim (e.g., impersonating the victim and posting inflammatory messages to bulletin boards and in chat rooms, causing viewers of that message to send threatening messages back to the victim "author.")

Electronic communications technologies also lower the barriers to harassment and threats; a cyberstalker does not need to physically confront the victim.

While there are many similarities between offline and online stalking, the Internet and other communications technologies provide new avenues for stalkers to pursue their victims.

A cyberstalker may send repeated, threatening, or harassing messages by the simple push of a button; more sophisticated cyberstalkers use programs to send messages at regular or random

intervals without being physically present at the computer terminal. California law enforcement authorities say they have encountered situations where a victim repeatedly receives the message "187" on their pagers - the section of the California Penal Code for murder. In addition, a cyberstalker can dupe other Internet users into harassing or threatening a victim by utilizing Internet bulletin boards or chat rooms. For example, a stalker may post a controversial or enticing message on the board under the name, phone number, or e-mail address of the victim, resulting in subsequent responses being sent to the victim. Each message -- whether from the actual cyberstalker or others -- will have the intended effect on the victim, but the cyberstalker's effort is minimal and the lack of direct contact between the cyberstalker and the victim can make it difficult for law enforcement to identify, locate, and arrest the offender.

#### Actual Cyberstalking Incidents

In the first successful prosecution under California's new cyberstalking law, prosecutors in the Los Angeles District Attorney's Office obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances. The defendant terrorized his 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized of being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her. The former security guard pleaded guilty in April 1999 to one count of stalking and three counts of solicitation of sexual assault. He faces up to six years in prison.

A local prosecutor's office in Massachusetts charged a man who, utilizing anonymous remailers, allegedly engaged in a systematic pattern of harassment of a co-worker, which culminated in an attempt to extort sexual favors from the victim under threat of disclosing past sexual activities to the victim's new husband.

An honors graduate from the University of San Diego terrorized five female university students over the Internet for more than a year. The victims received hundreds of violent and threatening e-mails, sometimes receiving four or five messages a day. The graduate student, who has entered a guilty plea and faces up to six years in prison, told police he committed the crimes because he thought the women were laughing at him and causing others to ridicule him. In fact, the victims had never met him.

The anonymity of the Internet also provides new opportunities for would-be cyberstalkers. A cyberstalker's true identity can be concealed by using different ISPs and/or by adopting different screen names. More experienced stalkers can use anonymous remailers that make it all-but-impossible to determine the true identity of the source of an e-mail or other electronic communication. A number of law enforcement agencies report they currently are confronting cyberstalking cases involving the use of anonymous remailers.

Anonymity leaves the cyberstalker in an advantageous position. Unbeknownst to the target, the perpetrator could be in another state, around the corner, or in the next cubicle at work. The perpetrator could be a former friend or lover, a total stranger met in a chat room, or simply a teenager playing a practical joke. The inability to identify the source of the harassment or threats could be particularly ominous to a cyberstalking victim, and the veil of anonymity might encourage the perpetrator to continue these acts. In addition, some perpetrators, armed with the knowledge that their identity is unknown, might be more willing to pursue the victim

at work or home, and the Internet can provide substantial information to this end. Numerous websites will provide personal information, including unlisted telephone numbers and detailed directions to a home or office. For a fee, other websites promise to provide social security numbers, financial data, and other personal information.

### *Evidence suggests cyberstalking is a growing problem*

Although there is no comprehensive, nationwide data on the extent of cyberstalking in the United States, some ISPs compile statistics on the number and types of complaints of harassment and/or threats involving their subscribers, and individual law enforcement agencies have compiled helpful statistics. There is, moreover, a growing amount of anecdotal and informal evidence on the nature and extent of cyberstalking.

First, data on offline stalking may provide some insight into the scope of the cyberstalking problem. According to the most recent National Violence Against Women Survey, which defines stalking as referring to instances where the victim felt a high level of fear,<sup>(3)</sup>

- In the United States, one out of every 12 women (8.2 million) and one out of every 45 men (2 million) have been stalked at some time in their lives.
- One percent of all women and 0.4 percent of all men were stalked during the preceding 12 months.
- Women are far more likely to be the victims of stalking than men - nearly four out of five stalking victims are women. Men are far more likely to be stalkers - 87 percent of the stalkers identified by victims in the survey were men.
- Women are twice as likely as men to be victims of stalking by strangers and eight times as likely to be victims of stalking by intimates.

In the United States, there are currently more than 80 million adults and 10 million children with access to the Internet. Assuming the proportion of cyberstalking victims is even a fraction of the proportion of persons who have been the victims of offline stalking within the preceding 12 months, there may be potentially tens or even hundreds of thousands of victims of recent cyberstalking incidents in the United States.<sup>(4)</sup> Although such a "back of the envelope" calculation is inherently uncertain and speculative (given that it rests on an assumption about very different populations), it does give a rough sense of the potential magnitude of the problem.

Second, anecdotal evidence from law enforcement agencies indicates that cyberstalking is a serious - and growing - problem. At the federal level, several dozen matters have been referred (usually by the FBI) to U.S. Attorney's Offices for possible action. A number of these cases have been referred to state and local law enforcement agencies because the conduct does not appear to violate federal law.

In addition, some local law enforcement agencies are beginning to see cases of cyberstalking. For example, the Los Angeles District Attorney's Office estimates that e-mail or other electronic communications were a factor in approximately 20 percent of the roughly 600 cases handled by its Stalking and Threat Assessment Unit. The chief of the Sex Crimes Unit in the Manhattan District Attorney's Office also estimates that about 20 percent of the cases handled by the unit involve cyberstalking. The Computer Investigations and Technology Unit of the New York City Police Department estimates that almost 40 percent of the caseload in the unit involves electronic threats and harassment -- and virtually all of these have occurred in the

past three or four years.

Third, ISPs also are receiving a growing number of complaints about harassing and threatening behavior online. One major ISP receives approximately 15 complaints per month of cyberstalking, in comparison to virtually no complaints of cyberstalking just one or two years ago.

Finally, as part of a large study on sexual victimization of college women, researchers at the University of Cincinnati conducted a national telephone survey of 4,446 randomly selected women attending two- and four-year institutions of higher education. The survey was conducted during the 1996-97 academic year. In this survey, a stalking incident was defined as a case in which a respondent answered positively when asked if someone had "repeatedly followed you, watched you, phoned, written, e-mailed, or communicated with you in other ways that seemed obsessive and made you afraid or concerned for your safety." The study found that 581 women (13.1 percent) were stalked and reported a total of 696 stalking incidents; the latter figure exceeds the number of victims because 15 percent of the women experienced more than one case of stalking during the survey period. Of these 696 stalking incidents, 166 (24.7 percent) involved e-mail. Thus, 25 percent of stalking incidents among college women could be classified as involving cyberstalking.<sup>(5)</sup>

## **Current Efforts to Address Cyberstalking**

### *The law enforcement response*

Cyberstalking is a relatively new challenge for most law enforcement agencies. The first traditional stalking law was enacted by the state of California in 1990 - less than a decade ago. Since that time, some law enforcement agencies have trained their personnel on stalking and/or established specialized units to handle stalking cases. Nonetheless, many agencies are still developing the expertise and resources to investigate and prosecute traditional stalking cases; only a handful of agencies throughout the country have focused attention or resources specifically on the cyberstalking problem.<sup>(6)</sup>

### **Law enforcement response: awareness and training are key factors**

Based on recent informal surveys of law enforcement agencies, it appears that the majority of agencies have not investigated or prosecuted any cyberstalking cases. However, some agencies - particularly those with units dedicated to stalking or computer crime offenses - have large cyberstalking caseloads. As noted above, the New York Police Department's Computer Investigation and Technology Unit and the Los Angeles District Attorney's Stalking and Threat Assessment Team estimate that 40 and 20 percent of their caseloads, respectively, involve cyberstalking-type cases.

"Cyberspace has become a fertile field for illegal activity. By the use of new technology and equipment which cannot be policed by traditional methods, cyberstalking has replaced traditional methods of stalking and harassment. In addition, cyberstalking has led to offline incidents of violent crime. Police and prosecutors need to be aware of the escalating numbers of these events and devise strategies to resolve these problems through the criminal justice system."

Linda Fairstein

Chief of Sex Crimes Prosecution Unit

Manhattan District Attorney's Office

The disparity in the activity level among law enforcement agencies can be attributed to a number of factors. First, it appears that the majority of cyberstalking victims do not report the conduct to law enforcement, either because they feel that the conduct has not reached the point of being a criminal offense or that law enforcement will not take them seriously. Second, most law enforcement agencies have not had the training to recognize the serious nature of cyberstalking and to investigate such offenses. Unfortunately, some victims have reported that rather than open an investigation, a law enforcement agency has advised them to come back if the cyberstalkers confront or threaten them offline. In several instances, victims have been told by law enforcement simply to turn off their computers.

#### **Law Enforcement: Lack of Training and Expertise Can Frustrate Victims, Hinder Response**

A recent incident demonstrates how the lack of law enforcement training and expertise can frustrate cyberstalking victims: A woman complained to a local police agency that a man had been posting information on the web claiming that her nine-year-old daughter was available for sex. The web posting included their home phone number with instructions to call 24 hours a day. They received numerous calls. The couple reported the problem to the local police agency on numerous occasions, but the agency simply advised the couple to change their home phone number. Subsequently, the couple contacted the FBI, which opened an investigation. It was discovered that the local police agency did not have a computer expert, and the investigative officer had never been on the Internet. The local agency's lack of familiarity and resources may have resulted in a failure to understand the seriousness of the problem and the options available to law enforcement to respond to such problems.

Another indication that many law enforcement agencies underestimate the magnitude of the cyberstalking problem is the wide disparity in reported cases in different jurisdictions across the country. For example, one state attorney general's office in a midwestern state indicated that it received approximately one inquiry a week regarding cyberstalking cases and that it is aware of approximately a dozen prosecutions last year alone. In contrast, the state attorney general's offices in neighboring states indicated they have never received an inquiry into this type of behavior. Although one would generally expect some disparity in differing jurisdictions, the size of the disparity suggests that some law enforcement agencies do not have the training or expertise to recognize the magnitude of the problem in their jurisdictions.

**Law enforcement response: jurisdictional and statutory limitations may frustrate some**

## agencies

Some state and local law enforcement agencies also have been frustrated by jurisdictional limitations. In many instances, the cyberstalker may be located in a different city or state than the victim making it more difficult (and, in some cases, all but impossible) for the local authority to investigate the incident. Even if a law enforcement agency is willing to pursue a case across state lines, it may be difficult to obtain assistance from out-of-state agencies when the conduct is limited to harassing e-mail messages and no actual violence has occurred. A number of matters have been referred to the FBI and/or U.S. Attorney's offices because the victim and suspect were located in different states and the local agency was not able to pursue the investigation.

The lack of adequate statutory authority also can limit law enforcement's response to cyberstalking incidents. At least 16 states have stalking statutes that explicitly cover electronic communications,<sup>(2)</sup> and cyberstalking may be covered under general stalking statutes in other states. It may not, however, meet the statutory definition of stalking in the remainder. In many cases, cyberstalking will involve threats to kill, kidnap, or injure the person, reputation, or property of another, either on or offline and, as such, may be prosecuted under other federal or state laws that do not relate directly to stalking.

Finally, federal law may limit the ability of law enforcement agencies to track down stalkers and other criminals in cyberspace. In particular, the Cable Communications Policy Act of 1984 (CCPA) prohibits the disclosure of cable subscriber records to law enforcement agencies without a court order and advance notice to the subscriber. See 47 U.S.C. 551(e), (h). As more and more individuals turn to cable companies as their ISPs, the CCPA is posing a significant obstacle to the investigation of cybercrimes, including cyberstalking. For example, under the CCPA, a law enforcement agency investigating a cyberstalker who uses a cable company for Internet access would have to provide the individual notice that the agency has requested his/her subscriber records, thereby jeopardizing the criminal investigation. While it is appropriate to prohibit the indiscriminate disclosure of cable records to law enforcement agencies, the better approach would be to harmonize federal law by providing law enforcement access to cable subscriber records under the same privacy safeguards that currently govern law enforcement access to records of electronic mail subscribers under 18 U.S.C. 2703. Moreover, special provisions could be drafted to protect against the inappropriate disclosure of records that would reveal a customer's viewing habits.

### **Law enforcement response: the challenge of anonymity**

Another complication for law enforcement is the presence of services that provide anonymous communications over the Internet. To be sure, anonymity provides important benefits, including protecting the privacy of Internet users. Unfortunately, cyberstalkers and other cybercriminals can exploit the anonymity available on the Internet to avoid accountability for their conduct.

Anonymous services on the Internet come in one of two forms: the first allows individuals to create a free electronic mailbox through a web site. While most entities that provide this service request identifying information from users, such services almost never authenticate or otherwise confirm this information. For these services, payment is typically made in advance through the use of a money order or other non-traceable form of payment. As long as payment is received in advance by the ISP, the service is provided to the unknown account holder. The

second form comprises mail servers that purposefully strip identifying information and transport headers from electronic mail. By forwarding mails through several of these services serially, a stalker can nearly perfectly anonymize the message. The presence of both such services makes it relatively simple to send anonymous communications, while making it difficult for victims, providers, and law enforcement to identify the person or persons responsible for transmitting harassing or threatening communications over the Internet.

### **Law enforcement response: specialized units show promise in combating cyberstalking**

A growing number of law enforcement agencies are recognizing the serious nature and extent of cyberstalking and taking aggressive action to respond. Some larger metropolitan areas, such as Los Angeles and New York, have seen numerous incidents of cyberstalking and have specialized units available to investigate and prosecute these cases. For example, Los Angeles has developed the Stalking and Threat Assessment Team. This team combines special sections of the police department and district attorney's office to ensure properly trained investigators and prosecutors are available when cyberstalking cases arise. In addition, this specialized unit is given proper resources, such as adequate computer hardware and advanced training, which is essential in investigating and prosecuting these technical cases. Similarly, the New York City Police Department created the Computer Investigation and Technology Unit. This unit provides regular training for police officers and prosecutors regarding the intricacies of cyberstalking investigations and prosecutions. The training includes understanding how chat rooms operate, how to obtain and preserve electronic evidence, and how to draft search warrants and subpoenas.

The programs in New York and Los Angeles both ensure that enforcement personnel receive proper training and have adequate resources to combat cyberstalking. Other jurisdictions are also taking steps to combat cyberstalking. One of the critical steps is learning how to trace communications sent over computers and the Internet. Traditional law enforcement techniques for surveillance, investigation, and evidence gathering require modification for use on computer networks and often require the use of unfamiliar legal processes. Law enforcement at all levels must be properly trained to use network investigative techniques and legal process while protecting the privacy of legitimate users of the Internet. These techniques are similar to those used in investigating other types of computer crime. Just as a burglar might leave fingerprints at the scene of a crime, a cyberstalker can leave an "electronic trail" on the web that properly trained law enforcement can follow back to the source. Thus, technological proficiency among both investigators and prosecutors is essential.

At present, there are numerous efforts at the federal and state levels that focus solely on high technology crimes. These units do not focus on cyberstalking alone, but they have the necessary expertise in computers and the Internet to assist in the investigation of cyberstalking when it arises. For example, the Federal Bureau of Investigation (FBI) has Computer Crime Squads throughout the country, as well as the National Infrastructure Protection Center in Washington, to ensure cybercrimes are properly investigated. Additionally, they have Computer Analysis and Response Teams to conduct forensics examinations on seized magnetic media. Similarly, in 1996 the Justice Department established the Computer Crime and Intellectual Property Section within the Criminal Division. These units have highly trained personnel who remain on the cutting edge of new technology and investigative techniques. In addition, each U.S. Attorney's office contains experienced computer crime prosecutors. These individuals -- Computer and Telecommunications Coordinators -- assist in the investigation and prosecution of a wide variety of computer crimes, including cyberstalking. In addition, at

the state level, several attorneys general have established special divisions that focus on computer crimes.

Although high-tech expertise is essential, police and prosecutors have developed other strategies for helping victims of cyberstalking. An Assistant U.S. Attorney reported that in two recent cases of e-mail harassment, he asked an FBI agent to confront the would-be harasser. The agent advised that such behavior might constitute a criminal offense. In both instances, the harassment stopped. Such strategies, however, are no substitute for prosecution under federal or state law in the appropriate circumstances.

A critical step in combating cyberstalking is understanding stalking in general. In many instances, cyberstalking is simply another phase in an overall stalking pattern, or it is regular stalking behavior using new, high-technology tools. Thus, strategies and techniques that have been developed to combat stalking in general often can be adapted to cyberstalking situations. Fortunately, many state and local law enforcement agencies have begun to focus on stalking, and some have developed special task forces to deal with this problem. In addition, the Attorney General submits an annual report to Congress entitled "Stalking and Domestic Violence." This report compiles valuable information about what the Department of Justice has learned about stalking and stalkers and is a valuable resource for law enforcement agencies and others.<sup>(8)</sup>

Cyberstalking is expected to increase as computers and the Internet become more popular. Accordingly, law enforcement at all levels must become more sensitive to cyberstalking complaints and devote the necessary training and resources to allow proper investigation and prosecution. By becoming technologically proficient and understanding stalking in general, agencies will be better prepared to respond to cyberstalking incidents in their jurisdictions. In addition, state and local agencies can turn to their local FBI or U.S. Attorney's office for additional technical assistance. Also, computer crime units and domestic violence units should share information and expertise, since many cyberstalking cases will include elements of both computer crime and domestic violence. Finally, law enforcement must become more sensitive to the fear and frustration experienced by cyberstalking victims. Proper training should help in this regard, but law enforcement at all levels should take the next step and place special emphasis on this problem. Computers and the Internet are becoming indispensable parts of America's culture, and cyberstalking is a growing threat. Responding to a victim's complaint by saying "just turn off your computer" is not acceptable.

### *Industry efforts*

Although the Internet industry has tried to combat abusive electronic communications overall, the industry as a whole has not addressed cyberstalking in particular. According to a review conducted as part of the preparation of the report, most major ISPs have established an address to which complaints of abusive or harassing electronic mail can be sent (generally, this address is "abuse@[the ISP's domain]" -- for example, "[abuse@aol.com](mailto:abuse@aol.com)"). In addition, these providers almost uniformly have provisions in their online agreements specifically prohibiting abusive or harassing conduct through their service and providing that violations of the policy will result in termination of the account.

In practice, however, ISPs have focused more on assisting their customers in avoiding annoying online behavior, such as receiving unsolicited commercial electronic mail ("spamming") or large amounts of electronic mail intentionally sent to an individual

("mail-bombing"); relatively less attention has been paid to helping victims of cyberstalking or other electronic threats. For some ISPs, the procedures for lodging complaints of online harassment or threats were difficult to locate, and their policies about what does or does not constitute a violation of service agreements were generally unhelpful. In addition, many ISPs do not inform their customers about what steps, if any, the ISP has taken to follow-up on their customer's complaint. These problems -- hard-to-locate complaint procedures, vague policies about what does and does not constitute prohibited harassment, and inadequate follow-up on complaints -- may pose serious obstacles to cyberstalking victims who need help.

Online industry associations respond that providing such protection to their customers is costly and difficult. Although they recognize that larger ISPs have begun to commit resources to dealing with harassment online, they caution that the costs of imposing additional reporting or response obligations upon ISPs may make it difficult for small or entrepreneurial ISPs to continue providing service at competitive rates. For example, the Commercial Internet Exchange, whose members carry approximately 75 percent of U.S. backbone traffic, cautions that no attempt to impose reporting requirements should be made unless fully justified by the record. However, according to the same group, the decentralized nature of the Internet would make it difficult for providers to collect and submit such data. Accordingly, the evidence of the scope of the cyberstalking problem is likely to remain for the foreseeable future defined primarily by anecdotal evidence, with no basis to determine whether the phenomenon is growing, static, or declining.

#### **Industry efforts: educating and protecting consumers**

Despite the difficulty in fully defining the scope of the cyberstalking problem, however, industry has made notable efforts to inform consumers about ways to protect themselves online. Such information is principally focused on protecting children and consumers on the Internet. For example, since 1996, the Internet Alliance, one of the key Internet industry groups, has worked with the Federal Trade Commission and government agencies on Project OPEN (Online Public Education Network). Project OPEN provides information about fraud, parental controls, and protecting privacy.<sup>(9)</sup> Although this information is not specifically relevant to cyberstalking, much of the advice about protecting children and safeguarding privacy while online may be of assistance to individuals who want to use the Internet while protecting against potential cyberstalkers. More recently, a number of industry organizations have joined together to develop, GetNetWise.Com - a single, comprehensive online resource to help parents and children use the Internet in a safe and educational manner.

Other similar industry efforts have recently been announced to address other aspects of computer-related crime. For example, the Department of Justice and the Information Technology Association of America (ITAA) announced the Cybercitizen Partnership in March 1999. This partnership is intended to boost cooperation between industry and government, expand public awareness of computer crime issues among children and adolescents, and provide resources for government to draw upon in addressing computer crime. The industry has also responded to the complaints of parents who are worried about the content available to their children over the Internet by announcing the "One Click Away" initiative to give parents important information about protecting their children in a central location. Similar education and outreach efforts, approached through cooperation between industry and government, may educate individuals concerned about these issues and therefore mitigate some of the dangers of cyberstalking.

In addition, other Internet industry sectors have begun to address aspects of the cyberstalking problem. Many of these solutions focus on the ability of individuals to protect themselves against unwanted communications. For example, most Internet "chat" facilities offer users the ability to block, squelch, or ignore chat messages or "paging" from individuals who are attempting to annoy or threaten them. Similarly, many e-mail users have tools which allow the users to block e-mail from individuals who are attempting to harass or annoy them. Such a solution may be useful in situations where the communications are merely annoying. Unfortunately, such a solution is less appropriate when threatening communications are received, because a victim who never "receives" the threat may not know they are being stalked, and may be alerted, for the first time, when the stalker shows up to act on the threat.

In another type of response, providers have begun to set up "gated communities" for individuals, families, and children. The techniques used by such communities are still in developmental stages, but they range from specialized servers, which allow potentially objectionable content to be filtered at the server, to designated areas for children and teens, which place restrictions on the amount or types of personal information that will be provided to others. Individuals who are concerned about being stalked may find refuge in such communities.

While these efforts all reflect important initiatives for self-protection, both industry and government representatives agree that a key component of addressing the cyberstalking problem is education and empowerment: If individuals are given clear direction about how to protect themselves against threatening or harassing communications, and how to report incidents when they do occur, both industry and law enforcement will be in a position to cooperate to conduct investigations.

#### **Industry efforts: cooperation with law enforcement**

Both industry and law enforcement benefit when crime over the Internet is reduced. In particular, the Internet industry benefits significantly whenever citizen and consumer confidence and trust in the Internet is increased. Accordingly, both industry and law enforcement recognize the need to cooperate more fully with one another in this area. Industry representatives have noted that contact between industry and law enforcement -- particularly in the area of harassment -- is sporadic and episodic. Industry representatives, who were consulted as part of the preparation of this report, indicated their willingness to participate in training efforts for law enforcement. Law enforcement -- particularly on the state and local level, who will often be first responders to cyberstalking complaints -- should be willing to engage industry in dialogue and take advantage of the expertise offered by industry in designing training programs. Moreover, closer cooperation between law enforcement and industry will help to ensure that law enforcement officers know who at the ISPs to call and how to proceed when they receive a complaint, and ISPs have a contact in law enforcement when they receive a complaint that warrants intervention by law enforcement.

#### ***Victims and support organizations***

Because cyberstalking is a relatively new criminal phenomenon, very little public attention and resources have been committed to addressing this crime. Consequently, victims of online harassment and threats, often in collaboration with victim service providers and advocates, have had to step in to fill the void by developing their own informal support networks and informational web sites to exchange information about how to respond to these crimes

effectively.

Victim service providers report that the Internet is rapidly becoming another weapon used by batterers against their victims. Just as in real life, abused women can be followed in cyberspace by their batterers, who may surreptitiously place their target under surveillance without her knowledge and use the information to threaten her or discredit her by putting misinformation on the Internet. Victim service providers recommend that victims make copies of all e-mails sent by the batterer as evidence of his stalking and advise a victim to let the stalker know that she does not want to have any further contact with him. SAFE House, a domestic violence victim service provider in Michigan, suggests that victims change their passwords often; refrain from telling anyone what the password is; do not use a password or other identifying information that the batterer/stalker can guess; set up a program that requires a password even to get on the computer; be sure to clear out the history information if programs such as ICQ, AOL Communicator, and Excite PAL, are used; remember that many chat rooms have archives that can be accessed later on by anyone; be careful about what is said in chat rooms and use an alias that is only known to good friends; be aware that if the screen name of the assailant is known, he can be blocked from tracking victims through a buddy list on AOL; and, consult the ISP about the best way to secure their account.

A focus group convened on October 30, 1998, by the Office for Victims of Crime, a component within the U.S. Department of Justice, sought to identify the needs of stalking victims, including victims whose stalkers used the Internet to track and to harass their victims. The victims at the focus group emphasized that although the response of law enforcement and victim service providers is important, stalking victims need a wide range of services from doctors, mental health providers, day care providers, welfare and child protection workers, school staff, and employers. In addition, the focus group participants indicated that community awareness and understanding of what constitutes stalking behavior is critical to the support and well-being of stalking victims. Finally, all of the stalking victims reported that the consequences of not being believed or supported, or having their fears viewed as exaggerated or unrealistic, can be devastating. Some victims feel isolated and alone, are made to believe that the stalking is their fault, lose primary relationships, or fear losing their jobs. These issues are just as relevant to cyberstalking victims as they are to victims of offline stalking.

### **Adequacy of Existing Laws**

Although stalking has been a problem for many years, only in this decade has it received significant attention from lawmakers, policy officials, and law enforcement agencies. In 1990, California became the first state to enact a specific stalking law. Since that time, all 50 states and the District of Columbia have enacted stalking laws.

### ***State cyberstalking laws***

Less than one third of the states have anti-stalking laws that explicitly cover stalking via the Internet, e-mail, pagers, or other electronic communications. California, for example, only recently amended its stalking statute to cover cyberstalking. This law was used in the prosecution of a 50-year-old former security guard who pleaded guilty on April 28, 1999, to one count of stalking and three counts of solicitation of sexual assault after using the Internet to solicit the rape of a woman who rejected his romantic advances. While the general stalking statutes in some states may cover cyberstalking, all states should review their laws to ensure they prohibit and provide appropriate punishment for stalking via the Internet and other

electronic communications.

### *Federal cyberstalking laws*

Federal law provides a number of important tools that are available to combat cyberstalking. Under 18 U.S.C. 875(c), it is a federal crime, punishable by up to five years in prison and a fine of up to \$250,000, to transmit any communication in interstate or foreign commerce containing a threat to injure the person of another. Section 875(c) applies to any communication actually transmitted in interstate or foreign commerce -- thus it includes threats transmitted in interstate or foreign commerce via the telephone, e-mail, beepers, or the Internet.

Although 18 U.S.C. 875 is an important tool, it is not an all-purpose anti-cyberstalking statute. First, it applies only to communications of actual threats. Thus, it would not apply in a situation where a cyberstalker engaged in a pattern of conduct intended to harass or annoy another (absent some threat). Also, it is not clear that it would apply to situations where a person harasses or terrorizes another by posting messages on a bulletin board or in a chat room encouraging others to harass or annoy another person (as in the California case, discussed *infra*).

Certain forms of cyberstalking also may be prosecuted under 47 U.S.C. 223. One provision of this statute makes it a federal crime, punishable by up to two years in prison, to use a telephone or telecommunications device to annoy, abuse, harass, or threaten any person at the called number.<sup>(10)</sup> The statute also requires that the perpetrator not reveal his or her name. See 47 U.S.C. 223(a)(1)(C). Although this statute is broader than 18 U.S.C. 875 -- in that it covers both threats and harassment -- Section 223 applies only to direct communications between the perpetrator and the victim. Thus, it would not reach a cyberstalking situation where a person harasses or terrorizes another person by posting messages on a bulletin board or in a chat room encouraging others to harass or annoy another person. Moreover, Section 223 is only a misdemeanor, punishable by not more than two years in prison.

The Interstate Stalking Act, signed into law by President Clinton in 1996, makes it a crime for any person to travel across state lines with the intent to injure or harass another person and, in the course thereof, places that person or a member of that person's family in a reasonable fear of death or serious bodily injury. See 18 U.S.C. 2261A. Although a number of serious stalking cases have been prosecuted under Section 2261A, the requirement that the stalker physically travel across state lines makes it largely inapplicable to cyberstalking cases.

Finally, President Clinton signed a bill into law in October 1998 that protects children against online stalking. The statute, 18 U.S.C. 2425, makes it a federal crime to use any means of interstate or foreign commerce (such as a telephone line or the Internet) to knowingly communicate with any person with intent to solicit or entice a child into unlawful sexual activity. While this new statute provides important protections for children, it does not reach harassing phone calls to minors absent a showing of intent to entice or solicit the child for illicit sexual purposes.

Thus, although current statutes address some forms of cyberstalking, there are gaps in current federal and state law. As outlined in the Recommendations below, States should review their existing stalking and other statutes to determine whether they address cyberstalking and, if not, expeditiously enact laws that prohibit cyberstalking.

Federal legislation also is needed to fill the gaps in current law. While most cyberstalking cases will fall within the jurisdiction of state and local authorities, there are instances - such as serious cyberharassment directed at a victim in another state or involving communications intended to encourage third parties to engage in harassment or threats - where state law is inadequate or where state or local agencies do not have the expertise or the resources to investigate and/or prosecute a sophisticated cyberstalking case. Therefore, federal law should be amended to prohibit the transmission of any communication in interstate or foreign commerce with intent to threaten or harass another person, where such communication places another person in fear of death or bodily injury to themselves or another person. Because of the increased vulnerability of children, the statute should provide for enhanced penalties where the victim is a minor. Such targeted, technology-neutral legislation would fill existing gaps in current federal law, without displacing the primary law enforcement role of state and local authorities and without infringing on First Amendment-protected speech.

### First Amendment and Other Legal Considerations

All 50 States, the District of Columbia, and the federal government have passed laws that criminalize stalking to address the serious harms and dangers that result from stalking, including the fear of violence and loss of privacy and control suffered by the victim. In addition to the direct harms caused by stalking is also frequently a precursor to physical violence against the victim. By its nature, however, stalking is not a crime that can be defined with a particularized, discrete set of acts. Frequently stalking consists of a course of conduct that may involve a broad range of harassing, intimidating, and threatening behavior directed at a victim. The conduct can be as varied as the stalker's imagination and ability to actions that harass, threaten, and force himself or herself into the life and consciousness of the victim. As new technologies become available, stalkers adapt those technologies to new ways of stalking victims. This is the case with the Internet and cyberstalking.

As a result of the breadth of conduct potentially involved in stalking, anti-stalking statutes need to be relatively broad to be effective. At the same time, however, because of that breadth and because stalking can involve expressive conduct and speech, anti-stalking statutes must be carefully formulated and enforced so as not to impinge upon speech that is protected by the First Amendment. This is particularly true with regard to cyberstalking laws, which frequently will involve speech over the Internet. The Internet, moreover, has been recognized as an important tool for protected speech activities. See, e.g. *Reno v. American Civil Liberties Union*, 521 U.S. 844, 850-52, 870 (1997); *American Civil Liberties Union v. Reno*, 31 F.Supp.2d 473, 476, 493 (E.D. Pa. 1999).

The fact that stalking behavior (including cyberstalking) may implicate important issues of free speech, however, does not eliminate the significant public interest in its criminal regulation or suggest that a criminal regulation would be prohibited by the freedom of speech guarantees of the First Amendment. The First Amendment does not prohibit any and all regulation that may involve or have an impact on speech. Of particular relevance to stalking, the Supreme Court has recognized that governments may criminalize true threats without violating the First Amendment. See, e.g., *Watts v. United States*, 394 U.S. 705 (1969) (per curiam). As discussed in the Introduction of this report, stalking (as well as cyberstalking) generally involves conduct reasonably understood to constitute a threat of violence, and such threats may be criminalized consistent with the First Amendment.

One of the recommendations in this report calls on states to review and update their statutes, where necessary, to cover electronic communications within their stalking laws. Care must be taken in drafting cyberstalking statutes to ensure that they are not so broad that they risk chilling constitutionally protected speech, such as political protest and other legitimate conduct. A carefully drafted statute can provide

speech, such as political protest and other legitimate conduct. A carefully drafted statute can provide broad protections against cyberstalking without running afoul of the First Amendment.

---

## **Recommendations**

### *General recommendations*

- The law enforcement community, private industry, victims assistance providers, and individuals must recognize that cyberstalking is a serious problem -- not only as a potential precursor to offline threats and violence, but also as a serious invasion of an increasingly important aspect of people's everyday lives. At the same time, it is important to note that many forms of annoying and menacing activity on the Internet do not rise to the level of illegal activity and are properly addressed by individuals and service providers without recourse to law enforcement channels.
- The lack of comprehensive data on the nature and extent of cyberstalking makes it difficult to develop effective response strategies. Future surveys and research studies on stalking should, where possible, include specific information on cyberstalking. Industry organizations can and should play a role not only in increasing the amount of data on the cyberstalking problem, but also ensuring that the data can be analyzed in a meaningful way.

### *Legislative recommendations*

- States should review their existing stalking and other statutes to determine whether they address cyberstalking and, if not, promptly expand such laws to address cyberstalking.
- Although State and local law enforcement agencies should retain primary jurisdiction over cyberstalking cases, federal law should be amended to address gaps in existing law where the conduct involves interstate or foreign communications. Such legislation should prohibit the transmission of any communication in interstate or foreign commerce with intent to threaten or harass another person where such communication places another in reasonable fear of death or bodily injury. Enhanced penalties should be available where the victim is a minor. Such legislation should be technology neutral and should apply to all forms of communication technologies.
- Federal law also should be amended to make it easier to track down stalkers and other criminals in cyberspace while maintaining safeguards for privacy. In particular, the Cable Communications Policy Act should be amended to provide access to the same type of subscriber records, and under the same standards and privacy safeguards, as those for electronic mail subscribers under 18 U.S.C. 2703 (while maintaining strict limits on access to records that reveal customer viewing habits).

### *Recommendations for law enforcement and criminal justice officials*

- Law enforcement agencies and courts need to recognize the serious nature of cyberstalking, including the close links between offline and online stalking.
- Law enforcement agencies need training on the nature and extent of the cyberstalking problem, including specific training on the legal tools available to address the problem, the need for, and effectiveness of, prompt action by law enforcement agencies, the most

effective techniques to investigate and prosecute cyberstalking crimes, and the resources available to cyberstalking victims.

- Law enforcement agencies with existing stalking or computer crime units should consider expanding the mission of such units to include cyberstalking, and law enforcement agencies that do not presently have a stalking section should consider expanding their capabilities to address this issue. At the least, law enforcement agencies should understand the patterns underlying stalking in general and be prepared to respond and intercede on behalf of cyberstalking victims.
- Law enforcement agencies should use mechanisms for quickly and reliably sharing information about cyberstalking incidents with other law enforcement agencies, thereby making it less likely that a cyberstalker can continue threatening behavior simply because neither the jurisdiction of the sender nor the jurisdiction of the victim believes that it can prosecute the offender.
- U.S. Attorneys' Offices, in consultation with other federal, state and local agencies, should examine the available resources and networks of investigators and prosecutors with the expertise to handle cyberstalking investigations. These include violent crime specialists, computer crime investigators and prosecutors, computer forensic specialists, and victim-witness coordinators, among others. The Law Enforcement Coordinating Committees, which have been established in each U.S. Attorneys' Office and are designed to foster coordination among law enforcement agencies, would be an appropriate body for addressing these issues.
- Law enforcement agencies should work more closely with victim groups to identify cyberstalking patterns and victims' experiences and to encourage cyberstalking victims to report incidents to law enforcement authorities.

### *Recommendations for the Internet and electronic communications industry*

The Internet and electronic communications industry should --

- Create an industry-supported website containing information about cyberstalking and what to do if confronted with this problem. Contact information for the major ISPs should be included so that Internet users can easily report cyberstalking cases after visiting this centralized resource. This recommendation could be implemented by expanding the "One Click Away" initiative or through a complementary but separate initiative focused on cyberstalking.
- Develop additional means to empower individuals to protect themselves against cyberstalking. Such means might include more accessible and effective filtering and blocking options. While some major ISPs already allow such options, others do not.
- Develop training materials designed specifically to assist law enforcement in the investigation and prosecution of cyberstalking and related crimes. For example, a short training video could be developed to increase awareness of the cyberstalking problem and to provide law enforcement officers with essential information on how to work with ISPs and others in the investigation of cyberstalking cases.
- Cooperate fully with law enforcement when investigating cyberstalking complaints. The

industry can do this, for example, by immediately freezing and retaining data for law enforcement use on any potential cyberstalking case.

- Establish best business practices to address illicit activity by terminating holders of fraudulent accounts.
- Sponsor an Internet Security and Law Enforcement Council of ISPs and other members of the Internet community to develop and promote industry best business practices relating to security and law enforcement issues (including cyberstalking), develop and distribute training materials for law enforcement on the investigation and prosecution of Internet crime, and promote more effective communication and cooperation between industry and law enforcement in combating online criminal activity.
- Establish and enforce clear policies that prohibit cyberstalking and related behaviors, including the termination of accounts for persons who violate such policies. While it appears that most of the larger ISPs have such policies, some smaller ISPs do not. Representatives from the Internet industry should consider establishing an industry-wide code of conduct that encourages all ISPs to adopt such procedures.
- Establish clear and understandable procedures for individuals - both customers and non-customers - to register complaints about individuals using the company's service to engage in cyberstalking. Such procedures should be easily accessible to individuals.
- Develop and widely disseminate educational materials to customers and others on how to protect themselves online.

#### *Recommendations for victim service providers and advocates*

Victim service providers and advocates should --

- Provide direct services and referrals to available resources that are specifically designed to assist victims of cyberstalking, or stalking in general where cyberstalking services are not available, and work to ensure that cyberstalking services are expanded to meet the needs of victims and enhance their safety;
- Train domestic violence and other victim service providers and advocates on Internet technology, the tactics used by cyberstalkers, and how to respond to the specific needs of cyberstalking victims;
- Name the behavior as cyberstalking and validate that a crime is occurring when working with individual victims;
- Serve as catalysts in community efforts to form partnerships among law enforcement, prosecution, the judiciary, the medical community and other community allies to address the specific safety needs of cyberstalking victims and hold offenders accountable for their actions;

- Raise public awareness about the devastating impact on cyberstalking victims of the tactics used by cyberstalkers and the steps that can be taken to prevent and combat this crime; and
- Inform public policy decision making.

### Appendix I: Cyberstalking Resources Online

**CyberAngels:** Non-profit group devoted to assisting victims of online harassment and threats, including cyberstalking. [www.cyberangels.org](http://www.cyberangels.org).

**GetNetWise:** Online resource for families and caregivers to help kids use the Internet in a safe and educational manner. Includes a guide to online safety, a directory of online safety tools, and directions for reporting online trouble. [www.getnetwise.org](http://www.getnetwise.org).

**International Association of Computer Investigative Specialists:** IACIS is an international volunteer non-profit corporation composed of law enforcement professionals dedicated to education in the field of forensic computer science. IACIS offers professional training to law enforcement agencies in a wide range of computer crime investigative techniques, provides an opportunity to network with other law enforcement officers trained in

computer forensics, and promotes research and development of specialized hardware and software to assist computer forensic professionals. [www.iacis.com](http://www.iacis.com).

**National Center for Victims of Crime:** The National Center for Victims of Crime (formerly known as the National Victim Center) provides referrals and advocacy services to victims through its toll-free national hotline. Through the hotline, victims are referred to the nearest, appropriate services in their community, including crisis intervention, assistance with the criminal justice process, and counseling and support groups. The National Center publishes bulletins on a number of topics, including domestic violence, sexual assault, and stalking. [www.ncvc.org](http://www.ncvc.org).

**National Cybercrime Training Partnership:** This interagency, federal/state/local partnership, led by the Department of Justice with extensive support from the Office of Justice Programs and the National White Collar Crime Center, is developing and delivering training to federal, state and local law enforcement agencies on the investigation and prosecution of computer crime. Information about the partnership can be found through the NWCCC website: [www.cybercrime.org](http://www.cybercrime.org).

**Privacy Rights Clearinghouse:** Nonprofit consumer information and advocacy program that offers consumers a unique opportunity to learn how to protect their personal privacy. PRC's services include a hotline for consumers to report privacy abuses and request information on ways to protect their privacy, fact sheets on privacy issues, including one entitled "Are You Being Stalked? Tips For Your Protection." [www.privacyrights.org](http://www.privacyrights.org).

**Search Group, Inc.:** SEARCH, the National Consortium for Justice Information and Statistics, provides assistance to state and local criminal justice agencies on a wide variety of information

technology issues. SEARCH, through its National Technical Assistance and Training Program, provides comprehensive, hands-on training on computer crime investigations at its headquarters in Sacramento, CA, and at regional training sites around the country. [www.search.org](http://www.search.org).

**Women Halting Online Abuse (WHOA):** Founded by women to educate the Internet community about online harassment, WHOA empowers victims of online harassment and develops voluntary policies that systems administrators can adopt to create an environment free of online harassment. WHOA educates the online community by developing website resources, including the creation of a safe-site and unsafe-site list to enable users to make informed decisions, and providing information about how users can protect themselves against harassment. [whoa.femail.com](http://whoa.femail.com).

## Appendix II: How You Can Protect Against Cyberstalking - And What To Do If You Are A Victim

### Prevention Tips

- \* Do not share personal information in public spaces anywhere online, nor give it to strangers, including in e-mail or chat rooms. Do not use your real name or nickname as your screen name or user ID. Pick a name that is gender- and age-neutral. And do not post personal information as part of any user profiles.
- \* Be extremely cautious about meeting online acquaintances in person. If you choose to meet, do so in a public place and take along a friend.
- \* Make sure that your ISP and Internet Relay Chat (IRC) network have an acceptable use policy that prohibits cyberstalking. And if your network fails to respond to your complaints, consider switching to a provider that is more responsive to user complaints.
- \* If a situation online becomes hostile, log off or surf elsewhere. If a situation places you in fear, contact a local law enforcement agency.

### What To Do If You Are Being Cyberstalked

- \* If you are receiving unwanted contact, make clear to that person that you would like him or her not to contact you again.
- \* Save all communications for evidence. Do not edit or alter them in any way. Also, keep a record of your contacts with Internet system administrators or law enforcement officials.
- \* You may want to consider blocking or filtering messages from the harasser. Many e-mail programs such as Eudora and Microsoft Outlook have a filter feature, and software can be easily obtained that will automatically delete e-mails from a particular e-mail address or that contain offensive words. Chat room contact can be blocked as well. Although formats differ, a common chat room command to block someone would be to type: /ignore <person's screen name> (without the brackets). However, in some circumstances (such as threats of violence), it may be more appropriate to save the information and contact law enforcement authorities.
- \* If harassment continues after you have asked the person to stop, contact the harasser's Internet

Service Provider (ISP). Most ISP's have clear policies prohibiting the use of their services to abuse another person. Often, an ISP can try to stop the conduct by direct contact with the stalker or by closing their account. If you receive abusive e-mails, identify the domain (after the "@" sign) and contact that ISP. Most ISP's have an e-mail address such as abuse@(domain name) or postmaster@(domain name) that can be used for complaints. If the ISP has a website, visit it for information on how to file a complaint.

\* Contact your local police department and inform them of the situation in as much detail as possible. In appropriate cases, they may refer the matter to state or federal authorities. If you are afraid of taking action, there are resources available to help you, Contact either:

- The National Domestic Violence Hotline, 800-799-SAFE (phone); 800-787-3224 (TDD)
- A local women's shelter for advice and support.

1. Statutes that require a showing of a "credible threat" may be problematic in the prosecution of stalking. Stalkers often do not threaten their victims overtly or in person; rather, they engage in conduct that, when taken in context, would cause a reasonable person to fear violence. In the context of cyberstalking, a credible threat requirement would be even more problematic because the stalker, sometimes unbeknownst to the victim, may be located a great distance away and, therefore, the threat might not be considered credible. The better approach, codified in the federal interstate stalking statute, 18 U.S.C. 2261A, is to prohibit conduct that places a person in reasonable fear of death or bodily injury.

2. Comparisons based on data currently available. The data for cyberstalking, as noted in the text of this report, is largely anecdotal and informal.

3. "Stalking in America: Findings from the National Violence Against Women Survey." U.S. Department of Justice, Office of Justice Programs, and Department of Health and Human Services, Center for Disease Control and Prevention, April 1998 (available at [www.usdoj.gov/ojp](http://www.usdoj.gov/ojp)).

4. The CyberAngels, a not-for-profit organization that assists victims of cybercrimes, including cyberstalking, using statistics from unspecified sources, estimates there are approximately 63,000 Internet stalkers and 474,000 victims worldwide. For additional information about this estimate, see the CyberAngles website at [www.cyberangels.org](http://www.cyberangels.org).

5. Fisher, B. S., F. T. Cullen, J. Belknap, and M. G. Turner, "Being Pursued: Stalking Victimization in a National Study of College Women." (From a forthcoming report on sexual violence against college women funded by the US Department of Justice, National Institute of Justice).

6. The information gathered on the issue of cyberstalking is largely anecdotal. It was gathered through informal surveys of state Attorneys General, U.S. Attorneys' Offices, and, to a lesser extent, local prosecutors' offices. Victim accounts were given voluntarily through outreach conducted by the Violence Against Women Office of the U.S. Department of Justice. In addition, the American Prosecutors Research Institute of the National District Attorneys' Association compiled a report with background information on cyberstalking, which provided valuable information on current law enforcement efforts.

7. These states are Alabama, Alaska, Arizona, California, Connecticut, Delaware, Hawaii, Illinois, Indiana, Maine, Massachusetts, Michigan, New Hampshire, New York, Oklahoma, and Wyoming. Arkansas and Maryland have enacted statutes that cover harassment via

electronic communications outside their stalking statutes.

8. Copies of "Stalking and Domestic Violence: The Third Annual Report to Congress Under the Violence Against Women Act" can be obtained by contacting the National Criminal Justice Reference Service, Box 6000, Rockville, MD 20849-6000--(800) 851-3420.

9. Other resources available to individuals wishing to protect themselves against cyberstalking are listed in Appendix I, *infra*.

10. The definition of the term "telecommunications device" in that section excludes "interactive computer services." The intent of the exclusion is to insulate the service provider from liability, but not to insulate an individual user from liability for his or her criminal behavior. Accordingly, the Department of Justice has taken the position and successfully argued that a modem was a telecommunications device within the meaning of the statute. Therefore, an individual who used a modem to connect to the Internet and harass an individual is likely to fall within the terms of the statute. See *American Civil Liberties Union v. Reno*, 929 F.Supp. 824, 829 n.5 (E.D. Penn. 1996), *aff'd*, 521 U.S. 844 (1997); *Apollomedia Corporation v. Reno*, 19 F.Supp.2d 1081 (N.D. Cal. 1998), *aff'd*, --- U.S. ---, 119 S.Ct. 1450 (U.S. Apr. 19, 1999).

---

Return to . . . [CCIPS home page](#) || [Justice Department home page](#)

---

*Updated page October 18, 1999*  
*usdoj-crm/mis/mdf*

---

---

# The Clinton Administration's Law Enforcement Strategy:

## Combating Crime with 21st Century Technology and Information



Taking Back Our Neighborhoods  
One Block at a Time

October 1999

---

## Executive Summary

President Clinton and Attorney General Reno, working with state, local and tribal law enforcement officials, have launched a major effort to help America's communities fight crime. Over the course of the past six years, the Clinton Administration has helped unite federal, state, tribal and local crime control efforts, directed new resources into local efforts for crime fighting and crime prevention, and worked hand-in-hand with local law enforcement and local communities. These efforts have paid off. Six years into this strategy, crime has dropped to its lowest level in a quarter of a century.

The Clinton Administration's crime fighting efforts are taking place at a time of rapid advances in technology. New technologies have generated innovative tools for law enforcement to detect illegal activity, conduct investigations, identify, locate, arrest and prosecute those who violate the law, and monitor convicted criminals. But new technologies have also bred a new kind of criminal activity: cybercrime – the use of computers and computer networks to commit crime. And, the new tools of the information age have created new challenges to protecting personal privacy. The Clinton Administration is working to prepare America's law enforcement agencies for the 21st Century by deploying new and effective crime fighting tools, working to control crime in cyberspace and limiting any adverse impact of new technologies on individual privacy.

Over the past six years, the Administration has developed and deployed new law enforcement technologies to federal, state and local law enforcement agencies. With the help of the federal government, many law enforcement agencies now use advanced technological tools to identify criminal suspects by their DNA, generally predict where criminal activity is likely to happen in time to prevent it, find criminals through a national system of computerized fingerprints and apprehend criminals more safely with less-than lethal weapons. The Administration has proposed to continue to put technology to work fighting crime with \$350 million for Fiscal Year (FY) 2000 to help police stay ahead of every generation of criminals every place crime occurs – from the street corner to cyberspace.

The Administration has developed new strategies to control the growing problem of cybercrime. In the past decade, more and more people around the globe have started logging on to the Internet. Since 1991, there has been over a 500 percent increase in the number of computer intrusions, with nearly 42 percent of American businesses reporting computer break-ins. The Administration has responded by working with Congress to pass tougher laws for cybercrime and by aggressively enforcing the criminal laws aimed at protecting people from crime on the Internet.

The Federal government has an essential role to play in the area of technology and crime. States and localities simply do not have the resources, training or expertise to develop advanced approaches to crime fighting technology on their own. Research and development, standards setting, and education and training are all conducted most efficiently and effectively at the national level. The Administration has stepped forward to meet this challenge, to establish this infrastructure and to provide states, tribes and localities with an ability to fight crime with technology at a level they simply could not achieve on their own.

Finally, as important as the new technology we develop is our own continuing commitment to safeguard the privacy of Americans. The Clinton Administration has put in place protections to assure that private information is secure.

The opportunities and the challenges for law enforcement in this new age of technology are tremendous. The Clinton Administration is working to ensure that all law enforcement agencies across the country are ready to meet this challenge.

## I. Harnessing New Technologies to Fight Crime

Over the course of the past century, advances in technology have made law enforcement more and more effective. The development of fingerprinting in the 1900s and of crime laboratories in the 1920s helped police solve what were unsolvable crimes. Using the two-way radio and automobiles in the 1930s, police could respond to more incidents in an hour than they could previously respond to in a whole day. In more recent decades, personal computers have allowed police to process greater amounts of information more quickly, and solve an even greater number of crimes. Now, through the leadership of the Clinton Administration, the nation is taking another giant technological step forward.

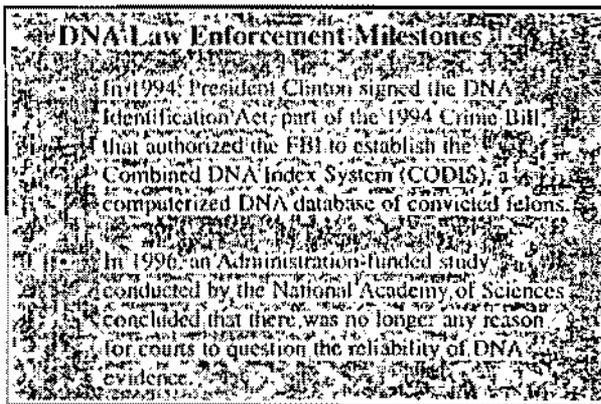
The Administration is helping states, localities and tribes to update and computerize their criminal history records to make sure they are fully accurate and accessible. It is also working to develop DNA identification technology to assist law enforcement in solving crimes – exonerating the innocent and convicting the guilty – in situations never before possible. At the same time, the Administration is transforming fingerprint identification into a faster, more effective law enforcement tool. By establishing several modern regional forensic laboratories, the Administration is using federal resources to make the most sophisticated crime fighting tools available to states, tribes and localities. And through development of new computer and communications technologies, the Administration has helped to link the communication and information systems of federal, state, local and tribal law enforcement agencies in ways that make them profoundly more efficient and effective at using information to prevent and solve crimes and to catch criminals. The Administration has also worked to develop, test and evaluate body armor and other devices that will save the lives of hundreds of law enforcement officers nationwide. The Administration has brought new technologies to state, local, and tribal law enforcement. And, federal law enforcement agencies, most notably the Department of Justice's Federal Bureau of Investigation (FBI), are also using these new technologies themselves in carrying out their law enforcement duties.

## Criminal History Records and Information Sharing

A basic building block in our use of technology to fight crime is computerization of state and federal criminal history records and the availability of this information to all law enforcement agencies. Criminals now routinely operate across state and national boundaries, requiring law enforcement to be able to quickly share information among jurisdictions to find fugitives, solve crimes, and adjudicate criminal cases. The Administration has taken a major leadership role in encouraging states, tribes and localities to modernize the way they collect information, enter it into computer databases and share it with other jurisdictions. Starting in 1995, the National Criminal History Improvement Program has provided more than \$273 million to state law enforcement agencies to improve, complete and standardize their record keeping. The Administration is creating a national network of information that allows local law enforcement to identify fugitives from justice, allows gun dealers to refuse sales to criminals convicted federally or in any state, allows courts to enforce child support orders issued in other jurisdictions, and allows state and local law enforcement to more easily collaborate to fight crime across state borders.

## DNA

Forensic DNA analysis has the potential to become as powerful an investigative tool for law enforcement in the 21st Century as fingerprints have been in this century. DNA, or deoxyribonucleic acid, carries the genetic code of each human being. Like fingerprints, each person's DNA is unique (except for identical twins). DNA is present in all cells and allows law enforcement to identify suspects by analyzing any blood, hair, skin, semen, or other biological material left at a crime scene. By comparing even microscopic amounts of evidence left at a crime scene with a sample of a known suspect, DNA can link criminals to their crimes with stunning accuracy. For example, DNA lifted from residual cells in the hatband of a baseball cap left at a murder scene enabled federal agents to identify the killer of an FBI agent.



Over the past six years, the Administration has made DNA technology more accessible to tribal, state and local police. We have developed and promulgated standards for quality control that state and local law enforcement can use to ensure that DNA evidence is accurate and persuasive in court. In 1998, the FBI implemented a national computer database of DNA profiles of convicted offenders and unknown suspects based on DNA samples from crime scenes. Instead of being limited to their own state databases, state and local agencies can now compare samples they obtain from crime scenes with DNA profiles already in the FBI database.

DNA evidence can also exonerate those wrongly accused or convicted of a crime. More than 65 people mistakenly convicted of felonies have been freed from prison on the basis of DNA evidence.

There is more work to be done to realize the full potential of this extraordinarily reliable method of linking criminals to their crimes. The Administration is seeking \$20 million in funding to build a national infrastructure for DNA evidence through a number of new initiatives.

- *Building a national DNA indexing system.* Recently, the FBI established a national DNA indexing system containing samples of DNA from 280,000 convicted criminals and from 6,500 crime scenes. The FBI is currently operating this system. Soon, more than 102 crime laboratories in 43 states will allow state

and local law enforcement to look for DNA matches, free of charge. Law enforcement agencies have also collected more than 650,000 additional DNA samples from convicted offenders and suspects, but those samples cannot be entered until they are analyzed. One of our major priorities is to complete the analysis of those 650,000 samples and have them entered and accessible through the national DNA indexing system. Much of the \$20 million the Administration has proposed for DNA infrastructure is for this project.

- *Improving DNA analysis.* The Administration is also working to refine techniques to analyze mitochondrial DNA. Mitochondrial DNA, because it is so plentiful in human cells, is even easier than other types of DNA to find at crime scenes. While this type of DNA does not uniquely identify individuals, it still has the potential to solve cases where the DNA is not available from whole living cells. This technology is currently used infrequently, but the additional resources the Administration is seeking to improve and advance the use of DNA evidence can reduce the cost and labor associated with mitochondrial DNA testing through refined analytical techniques.
- *Reducing the costs of and time required for DNA tests.* DNA tests are still fairly expensive. Also, it typically takes several days to process a DNA sample, and can take weeks or months to run the samples through the database. The Administration has just begun a five-year initiative to reduce the cost of DNA tests from \$700 a test to less than \$10 a test, to reduce the test time from hours to minutes and to increase the reliability of DNA evidence collected from even minute samples.

## Fingerprinting

Throughout most of this century, fingerprint evidence has been the most persuasive and conclusive type of evidence in court. DNA evidence is often

unavailable and is still in its infancy; so, when fingerprints are located, law enforcement count on them as the single most precise and accurate method of identifying potential suspects and other individuals.

The Clinton Administration has focused on improving the utility and reliability of fingerprint data. While fingerprints have been used as evidence for many years, there remain several problems with the collection, storage, and retrieval of fingerprint data. First, fingerprint evidence is not always easy for police to obtain. Most fingerprints are invisible to the naked eye, and law enforcement officials must use special techniques to transfer fingerprints from the crime scene to the evidence locker. Traditionally, police have lifted prints from crime scenes by dusting them with a special kind of powder that makes them visible, and then imprinting the visible image onto a piece of paper. Although obtaining fingerprints in this manner is reliable, the method has its limits – for example, police often have trouble lifting prints from uneven surfaces; once collected, police historically have stored fingerprints on index cards in file cabinets or have used other non-computerized storage, so that prints are not accessible to other agencies, or even other precincts; unless a suspect is already known, matching prints the traditional way is a tedious and time consuming chore because prints must be compared by hand. With the help of the Administration, these practices are being replaced by more efficient and effective fingerprint analysis.



Over the past six years, the Clinton Administration has developed and is implementing a comprehensive plan to improve fingerprinting technologies. This plan has three major elements:

- *Improving the methods of lifting prints at a crime scene.* New methods can produce reliable and useful results from older prints and partial prints. The Clinton Administration worked with Congress to obtain funding for improvements in the way law enforcement gathers and records fingerprints.
- *Promoting computerization of fingerprint files in local agencies.* Hundreds of state, local and tribal police departments have used federal funding to build a capacity to store, and more importantly, to match fingerprints in a computerized database. In these jurisdictions, police no longer search manually through fingerprint cards; instead, they can scan a crime scene print into the computer, and then search for a match. Since the 1980s, many states and localities have created computerized fingerprint databases, making it far easier to identify and help convict a suspect just by having the criminal's fingerprints.
- *Creating a national fingerprint database for use by police everywhere.* This database will permit police agencies anywhere in the country to compare a fingerprint lifted from a crime scene with the millions of prints on file with the FBI. The Administration is working to complete the development of one nationwide, integrated fingerprint database of major offenders, known as the Integrated Automated Fingerprint Identification System (IAFIS). This database was activated in July 1999. For FY 2000, the Administration has proposed \$70 million to enable the states to access the database, containing more than 34 million fingerprints, collected by federal, state, local and tribal agencies, of persons convicted of certain offenses under state,

federal and tribal law. The database, when completed, will be able to respond to electronic criminal fingerprint inquiries in two hours or less, and will cross-reference the suspects' criminal histories and outstanding arrest warrants, as well as stolen vehicle information. It is open around the clock, every day of the year. This is a vast improvement over past response times. The historic fingerprint backlog has been overtaken by technology advances.

### **Using Other Forensic Technologies and Building Modern Forensic Laboratories**

Fingerprints and DNA prints are not the only types of forensic evidence police use to identify criminals and solve crimes. For example, police can enhance security camera tapes to create a clearer picture or restore a seemingly inaudible tape recording. The FBI and the Department of the Treasury's Bureau of Alcohol, Tobacco and Firearms (ATF) can now create and store images of the identifying characteristics of bullet and cartridge casings collected from crime scenes. These images can be compared with previously collected images to link crimes. The FBI and the ATF are developing a system – the National Integrated Ballistics Identification Network (NIBIN) – that enables their previously independent databases to communicate, greatly increasing their information sharing capabilities and the likelihood of linking criminals to their crimes.

Through the efforts of the Clinton Administration, tribal, state, and local agencies have been able to upgrade their forensic laboratories and techniques. In 1994, the Administration funded the creation of several specialized technology centers across the country as well as four regional technology centers that provide forensic support to tribal, state and local agencies. The centers have helped police departments test crime scene evidence, obtain better forensic technology and train their personnel on how to use it.

The Administration has proposed new initiatives to further improve state, local, and tribal law enforcement technology capacity in FY 2000. The Administration is seeking \$10 million to continue the support of these technology centers and \$55 million in additional grant money to assist tribal, state and local police in improving their own forensic capabilities, including improvements in DNA testing.

### **Computer and Communications Technologies**

Computers and communication technologies have revolutionized day-to-day police work and made police more effective and more efficient. Computers have freed police from time-consuming administrative work and, as a result, police now have more time and better tools to patrol our streets and keep our neighborhoods safe.

**COMPUTERS.** Police work has traditionally involved a significant amount of paperwork – writing tickets and citations, filling out reports and booking suspects. With the development and availability of new technologies, police can enter information they collect at a crime scene directly into a laptop computer in their police car and send it electronically to the station for processing.

Computers can also be used to support electronic databases containing everything from fingerprints and DNA profiles to mug shots and criminal history records. The FBI's IAFIS database, for instance, already contains the associated criminal history for each of its over 34 million fingerprint profiles. Mug shots will be added to the database in the next year. Even with advances in recent years, however, there is still too much information in paper files, or on multiple, incompatible computer systems.

The Administration has funded programs to help state, local, and tribal law enforcement agencies computerize their operations. Under the COPS MORE program alone, part of the Administration's COPS program to place 100,000 additional officers on the streets in part by freeing them up from desk work, the Administration has provided over \$704 million in technology grants. With this program and others, agencies have been able to create automated booking procedures with digital cameras and special computer software. These programs, working in tandem with the National Criminal History Improvement Program, have also made funds available for updating and computerizing criminal history records. The Administration has funded projects to make data systems compatible, in order to facilitate the exchange

of information among police agencies. More recently, the Administration has taken a leading role in developing an integrated database that draws upon computerized information from all federal, state, local, and tribal criminal justice agencies – a single, “global” network of information. Ready access to this information resource, once it is online, will provide law enforcement officers the information they need, when they need it, wherever they need it, in the office or on the street.

The Administration is now proposing \$70 million for FY 2000 under COPS CONECT (Community Oriented Networking and Enhanced Communications Technology) to assist state, local and tribal agencies in purchasing laptop computers and networking software, \$50 million to those agencies for upgrading their criminal history records and crime identification technology systems, and another \$20 million toward the integration of these systems.

**CRIME MAPPING.** A new, cutting edge technology – crime mapping – allows law enforcement to link information about crimes with other information about a community, such as housing patterns, the transportation grid and traffic patterns, schools, recreation areas, police stations and businesses of all description. By combining this information with sophisticated computer analysis, crime mapping can be used to identify patterns of crime. Police can use these patterns to predict where and when crime is likely to occur again.

With this information, law enforcement agencies can focus their patrols in crime “hot spots” (areas where crime is especially concentrated), making it far more difficult for criminals to commit crimes. Crime mapping has been a great success in communities where it has been implemented, but most police agencies do not have access to this technology. Less than one-third of police departments with more than 100 officers – and less than three percent of smaller departments – are using computerized crime mapping technology today.



**Department of Justice  
Crime Mapping Programs**

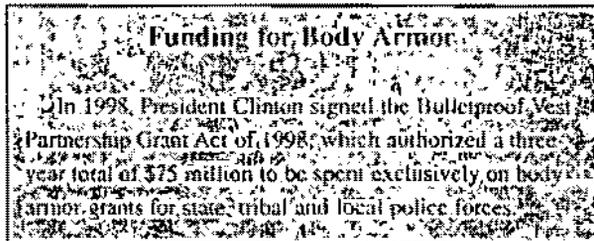
- COMPASS (Community Mapping, Planning, and Analysis for Safety Strategies) funding implementation of crime mapping strategies.
- COPS/MORE funding for technology and personnel as part of a program to place 30,000-50,000 more police on the streets with crime mapping technologies.
- Establishment of the Crime Mapping Research Center at the Department of Justice's National Institute of Justice.
- Establishment of CMAP (the Crime Mapping and Analysis Program) to provide technical assistance and training to tribal, state and local agencies for crime mapping and intelligence analysis.

The Administration is seeking \$30 million in FY 2000, and each year through 2004, to equip 22 communities with the most sophisticated crime mapping software currently available. This new program, called COMPASS, continues research and development already being undertaken by the Administration and will give local law enforcement an important tool to stop crime at the best time possible – before it happens.

**COMMUNICATIONS.** Ensuring public safety often requires effective coordination among many different public safety agencies. Every day, law enforcement officers are called upon to respond to crimes that cross jurisdictional lines. Currently, however, many law enforcement and other public agencies have incompatible communication systems. As a result, law enforcement officials from different agencies often cannot talk directly to one another over their radios. Public safety agencies discover – all too often during

an emergency – that they cannot mount a well-coordinated emergency response. Compatible communication systems not only ensure the delivery of more effective public safety services to communities, but also improve the safety and efficiency of law enforcement personnel.

The Administration is supporting interagency communications improvements. The Department of Justice has worked with industry manufacturers and other industry groups to develop standards for police radios to make sure that new systems are compatible with one another. The Administration has also helped state, local and tribal agencies' efforts to resolve their interoperability problems and funded their purchase of communication systems that meet standards for compatibility. Many of these efforts have been directed toward equipping these agencies with the latest wireless technology. The Administration has proposed \$80 million in FY 2000 to fund planning grants, as well as technical assistance and demonstration grants to states and tribes to advance this effort.



### Life-Saving Technologies

Law enforcement officers risk their lives every day to protect us, our families, and our communities. This is especially true when they are pursuing or confronting suspects. Recent advances in technology can greatly reduce the risk of injury. The Clinton Administration has taken a number of steps to make this technology available to federal, state, local and tribal law enforcement throughout the nation.

**PROTECTIVE BODY ARMOR.** The Administration has helped to ensure that federal, state, local and tribal

police officers have access to effective life saving body armor. The Departments of Justice and Defense have collaborated to develop body armor that is lighter and more easily concealed, but strong enough to withstand rifle and handgun bullets at close range. The Administration has also disseminated nationwide performance standards and a testing program for body armor. By developing these standards and testing over 1,500 models, the Administration has given smaller police agencies the information they need to make sure that the armor they buy is the best available. The Administration has also helped local police agencies purchase body armor. Body armor meeting these standards or purchased under this program has saved the lives of some 2,100 law enforcement personnel.

**HANDLING DANGEROUS SUSPECTS.** When apprehending a dangerous or armed criminal suspect, law enforcement officers have often had to choose between physically restraining the suspect (which is dangerous to the officers) and using their guns or batons to subdue the suspect (which is dangerous to the suspect). The Administration is committed to providing law enforcement tools to handle dangerous suspects while minimizing the risk of harm to police, the public and the suspect. Administration funded research is currently exploring a wide range of less-than-lethal weapon technologies – everything from pellet bags to capture nets. The Administration has also funded development of a tool, the retractable Road Spike™, to puncture the tires of a fleeing vehicle, inducing a slow and safe controlled stop and thus putting an end to a potentially dangerous high-speed chase.

### Federal Agencies Use of 21st Century Technologies

The Administration is committed to making 21st Century technology available to state, local, and tribal officials. At the same time, federal law enforcement agencies are using a wide range of new technologies to strengthen federal law enforcement capabilities.

**PROTECTING THE BORDER.** The Immigration and Naturalization Service (INS) and the U.S. Customs

Service are pioneering the use of many technologies in their efforts to protect our nation's borders. The INS is using fingerprinting technology to track border crossers so they can identify smugglers and criminal aliens returning illegally to the United States. The INS is also installing a computer-coordinated web of motion sensors and cameras to monitor stretches of the Mexico-U.S. border. Working together, INS and the Customs Service are remotely staffing key border crossings along the Canadian-American border with robotic cameras and remotely operated road blocking mechanisms. The U.S. Customs Service is now using both mobile and fixed site x-ray machines to check trucks and other large vehicles for contraband contained in hidden compartments.

To facilitate the smooth flow of legal vehicle traffic at ports of entry, the Administration has also begun to use a system that identifies legal vehicles electronically, and allows INS agents to verify visually occupants' identities by comparing the current occupants against digital images of those who are supposed to be traveling in the vehicle. At small northern border crossings, local residents can now use automated ports when staff are not on duty. These automated ports use video imaging to allow entry to local residents who are frequent low-risk border crossers in remote areas, but preventing entry of others in order to safeguard the integrity of the northern border. These new tools enhance enforcement and reduce fraudulent entry into the country.

**IMPROVING SECURITY AT FEDERAL PRISONS.** The Federal Bureau of Prisons has installed perimeter detecting systems and heartbeat detector systems to increase prison security, and has begun using "telemedicine," which brings medical treatment and evaluation to prison inmates from off-site hospitals, clinics or offices by video. Telemedicine lowers costs and lessens the chance of prisoner escape when inmates are transported from prisons to facilities for treatment. Video teleconferencing is being used by federal courts to conduct hearings while the prisoner remains in custody. This minimizes the risks of prisoner movement, protects law enforcement personnel and can expedite the hearing process. Federal authorities are

also using sophisticated electronic monitoring to supervise the activities and whereabouts of pre-trial detainees and parolees.

**HALTING COUNTERFEITING.** The Department of the Treasury is developing new anti-counterfeiting technologies, including the issue of redesigned, harder to copy currency, such as the new \$100, \$50, and \$20 bills. New \$10 and \$5 bills will be printed in the next few years.

**PROTECTING AGAINST TERRORISM.** The Administration has made the safety of government facilities and other high security sites a priority. Among other steps taken, the Secret Service has installed new sensors capable of detecting biochemical as well as traditional threats to high-security sites. The Administration is funding research to develop a type of personal alarm to be worn by law enforcement officers that monitors and alerts the officer to the presence of hazardous agents and the need to use special protective gear.

The FBI is also developing a system to exchange terrorist-related forensic data through secure telecommunications links that will allow forensic scientists from participating countries around the world to enter and retrieve data from three separate FBI forensic databases. This will make it easier for investigators to analyze data and identify suspects in international terrorism incidents. Historically, this exchange of information had to be conducted by mail or by diplomatic pouch. The ability of this system to store, retrieve and transmit forensic data rapidly, accurately and securely significantly will enhance international law enforcement capabilities in response to international terrorist incidents.

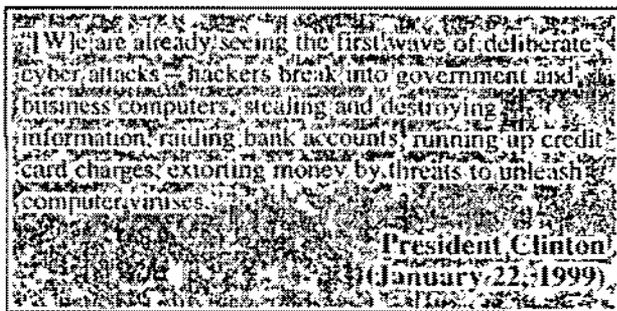
**SLOWING THE DRUG TRADE.** The Justice Department's Drug Enforcement Administration (DEA) is using technology to target the source of illegal drugs flowing into the United States, and to monitor the drug distribution networks within the states. In cooperation with foreign countries throughout the world, the DEA has created a database containing information regarding growing methods and soil components used in the

cultivation of drugs throughout the world. With this information, DEA agents can chemically analyze seized drugs and match those results with the database samples to identify where a particular shipment of drugs originated. The Department of Justice is also now able to track the movements of suspected drug dealers across state lines, which enables investigators to understand better the current distribution networks of the drug trade. Having this data allows law enforcement agents at all levels to target their resources most effectively to stop the influx of drugs into the United States.

## II. Fighting Cybercrime

Computers and the growth of the Internet have generated justifiable excitement over the past few years. The introduction of these new technologies has brought a new type of crime – cybercrime. Cybercrime generally has taken one of three forms.

First, computer criminals target computers for their offenses. With computer software that can break passwords, computer criminals have raided data files to steal inventions and other sensitive information, stolen money by illegally transferring it out of bank customers' accounts, and unleashed dangerous and devastating computer viruses that can do everything from distorting data to obliterating it, costing American businesses millions of dollars in delays and lost business opportunities and disrupting local, state and even federal government agencies. Recent studies confirm that this type of cybercrime is on the rise, with 30 percent of computer security professionals reporting that their computer systems were penetrated by outsiders.



The Administration has made it a priority to stop the proliferation of this type of cybercrime. The President signed both the National Information Infrastructure Protection Act of 1996, which protects the confidentiality, integrity, and availability of data and computer systems and the Economic Espionage Act of 1996, which extends the reach of the criminal law to the electronic theft of trade secrets. In addition, on February 27, 1998, the Attorney General announced the formation of the National Infrastructure Protection Center at FBI Headquarters in Washington, D.C. The Center is a joint government and private sector partnership, including representatives from the relevant agencies of federal, state and local governments and the private sector, created to address the daunting challenge of protecting the critical infrastructures on which our nation depends.

A second type of cybercrime that has emerged is the use of computers as tools to commit traditional crimes by engaging in activities that are heavily regulated or flatly prohibited both on and off the Internet, such as gambling, prostitution, the distribution of child pornography and the sale of prescription drugs, guns, and alcohol. The Administration has responded swiftly to this type of cybercrime as well. A large percentage of the cases now handled by the Department of Justice's Child Exploitation and Obscenity section are now Internet-related cases. The Department is also engaged in an Internet fraud initiative and intellectual property initiative, both of which focus on the use of the Internet to engage in traditional crimes. These initiatives will help to ensure that the Department has investigators and prosecutors who have the technical knowledge to address these offenses and who will increase the number of cases ultimately prosecuted. Law enforcement officials are also addressing the challenges posed by the recent proliferation of websites detailing how to commit a whole range of crimes – from how to make a bomb or hack into a computer to how to hire a hit man and get away with murder. The Department's efforts focus on cases involving the aiding and abetting or solicitation of criminal activity, and are carefully tailored so as not to chill First Amendment rights.

A third role of computers, often linked to cybercrime, involves computers which are used to store contraband or evidence of crime. Narcotics dealers, for example, may use personal computers to store records pertaining to drug trafficking instead of relying on old-fashioned ledgers. The Administration has collaborated with state, local, and tribal law enforcement agencies to develop procedures for collecting this type of computer based evidence. Law enforcement personnel need to know what hardware and software to seize, how to preserve the information contained in computers, how to access that information for investigative purposes, and how to make sure that computer evidence can be used against suspects at trial. Special techniques are needed to recover the damaged or deleted files that often provide critical evidence in electronic investigations.

The Administration has supported and enhanced the efforts of law enforcement to fight cybercrime. The Attorney General has made law enforcement capabilities to identify, investigate and stop cybercrime a priority and has fully supported the work of the Justice Department's dedicated computer crime units – the FBI's high-tech squads and the Computer Crime and Intellectual Property Section (CCIPS) within the Criminal Division. These specialized units work actively with other national and international government agencies and with the private sector to mount a unified, global response to the threats of cybercrime. Also, in early 1995, the Department of Justice initiated the Computer / Telecommunications Coordinator program, under which each of the 93 United States Attorney's Offices has designated at least one Assistant United States Attorney to serve as an in-house high-technology expert. CCIPS provides special training to these prosecutors on rapidly advancing technological and legal issues. With these and other efforts, the Administration has aggressively responded to cybercrime.

Cybercrime poses unique challenges to law enforcement. In cyberspace, criminals can mask their identities and remain anonymous. Moreover, encryption – temporary conversion of information into unreadable code – allows criminals to evade

interception of their communications and hide stored data in effective ways. Law enforcement must continue to develop its investigative activities and capabilities with proper regard for the privacy rights associated with online activities.

### III. Privacy

Advances in technology offer great promise for improving our ability to protect Americans from crime, but they can present new challenges to our personal privacy. Many valuable crime fighting technologies, if used improperly, could interfere with the privacy of law-abiding citizens. New technology increases the opportunity for unlawful access to confidential personal information using a computer and the Internet to do everything from simple snooping to outright "identity theft" – the act of stealing personal information from a computer database and using that information to make purchases or access sensitive information. In addition to the initiatives against cybercrime described earlier in this report, the Administration has taken steps to ensure that the public does not pay for the rise of technology with the loss of individual privacy.

In 1998, President Clinton issued an Executive Memorandum on Privacy. Attorney General Reno implemented the President's directive by forming a Privacy Council within the Department of Justice. This Council, made up of representatives from the relevant components of the Department, including the FBI, the DEA and the Office of Information and Privacy, evaluates proposed legislation for its impact on personal privacy, examines the impact of new law enforcement technologies on individual privacy, identifies new issues of and recommendations for privacy policy and ensures that the Department complies with the federal Privacy Act. The Department has also vigorously prosecuted cases where law enforcement overstepped its bounds and violated the Electronic Communications Privacy Act, which is designed to protect the privacy of telephone conversations and electronic communications.

The Attorney General's Privacy Council has also reviewed the Administration's efforts to ensure that as we develop DNA as a forensic tool, we also take care

---

that DNA databases are maintained in a manner that safeguards law-abiding citizens from intrusions of privacy. Some of the safeguards are that:

- DNA is collected only from known offenders and unknown suspects and not the general public;
- The portions of DNA used to identify persons reveal nothing about a person's physical characteristics, behavior, genetic diseases, or other private information; and
- Access to these databases is limited to law enforcement agents with the proper credentials.

The Administration also has taken the lead in protecting online privacy. Last year, President Clinton signed a bill that makes "identity theft" a crime. With stiffer penalties for federal crimes involving both fraud and a significant invasion of individual privacy, the Justice Department can now crack down on businesses

or individuals who engage in fraudulent schemes or steal people's identities. President Clinton has also convened an interagency working group to educate the public about the dangers of online crime, and to develop policies to protect online privacy. In sync with these efforts, the Department of Justice has made prosecution of crimes involving online invasions of privacy a priority.

## Conclusion

The Clinton Administration has taken significant steps to harness new technologies for law enforcement and to guard against the spread of crime in cyberspace. Many challenges still lie ahead. With the foundation established by the Administration's work and priorities in the 1990s, local, state and tribal governments and the federal government will enter the new millennium with a strong program to develop and deploy crime fighting technologies across the country and around the world. These tools will help make America safer in the 21st Century.

---

REMARKS OF THE HONORABLE JANET RENO  
ATTORNEY GENERAL OF THE UNITED STATES  
TO THE  
NATIONAL ASSOCIATION OF ATTORNEYS GENERAL

JANUARY 10, 2000

-----  
Stanford University, Dinkelspiel Auditorium

ATTORNEY GENERAL RENO: Thank you so much, Christine. And to all, I just salute you. I've had a chance now to visit so many different states to watch you in action, Democrats and Republicans, in a bipartisan way, do so much to serve people, not only of your own state, but of this nation. And one of the great points of honor for me has been the opportunity in these last seven years to serve with you. You are great public servants, and very special people, too.

Dean Sullivan, I thank you for your hospitality at this great law school. And, Christine, thank you for giving me this opportunity to speak at what I think is one of the most crucial conferences that I've heard about in a long time.

I come to you today to ask you to join with me to create a strong, permanent network of federal, state and local computer crime experts to do the following:

To share expertise and information technology, to assist each other 24 hours a day, seven days a week, around the clock, to prevent cybercrime wherever possible, and to bring those responsible for such crime, when it does occur, to justice;

To work with industry, the academic world and privacy groups to build trust and to protect our privacy and the Constitutional rights of all Americans;

And finally, to ensure that the Internet is a force that brings this world together and builds understanding across peoples and places and time.

I would invite you to meet with me in Washington at your earliest convenience to see how we can work with others -- with police, with prosecutors, with experts -- to forge such a network. For we are facing a moment in history where the decisions we make to confront the challenges of high technology and law enforcement are absolutely critical. These decisions will decisively shape our abilities to cope with crime for all time. The Internet and the revolution in information technology have transformed the world.

The monumental advances in computer software technology over the last ten years, combined with the explosive growth of the Internet, have changed the world forever. With breathtaking speed the Internet has nearly doubled in size every year since 1990. By 2003, the

number of Internet users worldwide is projected to be five hundred and two million people.

The Net has brought us splendid tools of wonder. Tools to improve the lives of people all over the world. Tools with which to learn and to teach. Tools with which to communicate with loved ones, with business associates. And as a great means and a great way for government to let its people know what it is doing.

A great example of the power of the Internet is the website for the families of the victims of Pan Am Flight 103. For these families are spread around the globe. But through a website they were able to access the latest developments in the case, reach out to the Office of Victims of Crime to answer their every question, to help them understand the Scottish legal system, and to communicate in private chat rooms with each other, to offer each other unparalleled support and understanding. Despite the great geographical divides that separate these families, the Internet has been a wonderful tool to bring them together and to offer them support at a time when they might otherwise be alone and afraid.

The Internet has provided us with tools to help sustain a vital economy, to generate business, promote commerce. And the volume of e-commerce is expected to grow from over \$100 billion dollars in 1999 to one trillion dollars in the year 2003.

The Net made Christmas shopping a lot easier for an awful lot of Americans this past year. It's promoted telecommuting and an opportunity for people to be with their families at greater measure. And it brings the world together, and it creates new bonds of understanding. It is a splendid tool of wonder.

But there is a dark side, a dark side of hacking, crashing networks, spreading viruses, which cause enormous loss. In a recent survey of Fortune 500 companies by the FBI and the Computer Security Institute found financial losses from computer crime exceeding \$360 million from '97 to '99. Of those responding to the survey, 62 percent reported computer security breaches within the last year.

And then there is terrorism. Our nation's infrastructures, including the banking system, the stock market, the electricity and water supply, telecommunications network, and critical government services such as emergency and national defense services, all rely on computer networks.

A real world terrorist, in order to blow up a dam, would need tons of explosives, a delivery system, and a surreptitious means with the aid of armed security guards. Cyber terrorists could achieve the same devastating result by hacking into the control network and opening the flood gates. There is a dark side. A dark side in terms of traditional crime, of threats, child pornography, fraud, gambling, stalking, and extortion.

They are all crimes that, when perpetrated via the Internet, can reach a larger and more accessible pool of victims, and can transform local scams into crimes that encircle the globe. By

connecting a worldwide network of users, the Internet has made it easier for wrongdoers to find each other, to congregate, to socialize, and to create an online community of support and social reinforcement for their antisocial behaviors.

And then there is hate and racism, bomb recipes, and insidious communications that tear up the privacy that we hold dear. Made all the more potent by the ease with which they can be accessed, and the concentrated forms that make this information more powerful and more devastating.

How do we ensure the wonderful promise of the Internet? How do we prevail against crime and terrorism on the Internet? How do we protect our privacy and ensure the Constitutional rights we cherish?

None of us can do this by going it alone. In the world of cybercrime, borders mean nothing. Interconnectivity of the information infrastructure means law enforcement, industry and the private sector must work together as never before. As never before in addressing a crime that can have such an impact on all of us. If we come together, if we come together as law enforcement, along with industry and the private sector and privacy groups, we can ensure the promise of the cyber revolution. If we don't, we give the cyber criminals and terrorists an advantage. There is no choice.

Let us all join together to form a strong, permanent network of experts dedicated to preventing computer crime and prosecuting those responsible. Washington likes to have letters, with the NIPC or the this or that or the other. Why don't we get rid of letters and just call it the Law Net.

I would like to talk about ten steps we must take, I think, to build a law net that can address the problems that we are concerned with. First, as I have indicated, we need to have a 24-hour, seven-day-a-week around the clock network of computer experts who assist each other in tracing and preventing and prosecuting cyber criminals effectively and efficiently. Why do we need this?

With the Internet, the criminal act appears on a computer in a specific location. But the criminal who put that criminal act on the computer could be next door, could be in the next state, could be halfway around the world. We must create and develop the ability to find that criminal and get to where he is in real time.

It doesn't take a master hacker to disappear on a network. For example, a hacker can leave his communications through a series of anonymous remailers, which advertise the fact that they keep no records. Or he can create a few forged e-mail headers with easy-to-use tools available on hacker websites. Or he can use a free trial account or two. Even a novice can effectively hide the trail of his communications and do it quickly.

This is an enormous challenge for law enforcement. For example, if a cyber stalker in

Palo Alto wants to send a threatening e-mail to someone in San Jose, he could easily route the message through hack accounts in New York, Argentina, and Japan before reaching his victim in San Jose.

Investigators in California tracing the message would have to contact service providers and government authorities in Manhattan, Buenos Aires, Kyoto just to track the cyber stalker back to Palo Alto. Tracing such a communication requires not only cooperation by government and industry officials in multiple jurisdictions, it also requires synchronized action and speed.

To combat these new challenges, we must create a system of interdependence, mutual reliability, information sharing, and most of all, integrated, effective connections. We must create an around-the-clock cybercrime network where each participating federal, state and local law enforcement agency designates an expert official to provide immediate assistance with cybercrime investigations to all other agencies in the network.

Questions of jurisdiction will arise: who handles what. I firmly believe in the principles of federalism. And in the principles of the federalism applied here, as in so many other instances, it will be state and local officials who will be pursuing the great bulk of this crime, according to principles of federalism. And we want to work out with you an appropriate understanding of who does what, where, all in the best interests of the people we serve.

The second step of this network involves a challenge for the Law Net, and it involves the development of an interactive secure way for state, local and federal authorities to share the latest techniques, the latest investigative information and intelligence on a secure online clearing house.

For example, if a group of victims complain to a state agency about a website in another jurisdiction, the clearing house website could help locate additional victims and notify authorities in the state where the website was posted.

This would foster cooperation and reduce the duplication of effort. Some existing law enforcement data bases could be used as building blocks for such a clearing house. We have already developed a nationally coordinated data base in the area of Internet crimes against children. And an Internet fraud complaint center is currently being developed by the cooperative efforts of the FBI and National White Collar Crime Center. The complaint center will go gather information about fraud schemes on the Net and forward written investigative reports concerning these schemes to the appropriate state and federal law enforcement agencies.

Let's explore that and make sure that we expand it in every way that is appropriate. And let us share research and development opportunities, both for our immediate needs and for the future. The technology in this area is changing right before our eyes. Unless we are there with the best scientists, the academic world, with industry, preparing for the future, we will find ourselves behind, no matter what we do.

The third area where I believe we have to share is in the utilization of expertise and training. I think this is probably one of the most precious commodities we have: somebody who knows the law, knows investigative techniques, and knows cyber issues.

Our population is catching up to the scientific development of these last 20 years, and the private sector salaries, plus the fact that the entire population has not become computer literate, makes it, as you all well know, very difficult to find and attract people into public service in this area.

That means we must share, must share our recruiting efforts and our training efforts. We must identify and inventory who is an expert in a particular subject matter and make that inventory available so that we don't have to hire 50 experts, but we can hire one for a particular subject to share that with our colleagues around the country.

I think it is imperative, too, that we train managers in how we build this network and how we interrelate together. Lawyers generally are not very good managers. And that makes us sometimes responsible for starting something and not planning it out very well. If we plan this network carefully and prudently, it can last for a long time to come.

I envision the network of contacts that extend from local detectives to the FBI, to the police forces abroad, from county prosecutors and DA's to state AG's, federal computer telecommunications coordinators, or CTC's, to the department's computer crime section and prosecutors in other countries.

We should have a clearing house that provides quick access to these experts. The computer crime and intellectual property section of the Department of Justice has begun to work on this model. They have a national training network of computer crime experts that developed by training assistant United States attorneys from each of the 94 districts across the country.

We call these experts CTC's. They are the resident expert in their district for computer crime cases. On complicated hacker cases, the secretary often will work with this nation-wide network to quickly bring criminals to justice. We want to join forces with the state AG's. And I understand that you have started to lay the groundwork for this effort, and we want to work with you in every way possible.

I know that some of you are well ahead of the curve in addressing this problem with high-tech crime units and among other states; Massachusetts, Michigan, New Jersey, New York, Nevada and Pennsylvania. And I'm told that we can learn a lot from those states. However we proceed, I want to work with you in every way possible to share the expertise.

The next issue is, we've got to learn how to share our equipment and technology. It makes no sense, if we have a gadget that costs a million dollars, for every state to have to buy the same gadget if we only need it about 25 percent of the time. Let's figure out, in a time where these pieces of equipment are so costly and where they become obsolete right before our eyes,

how we can use our dollars as wisely as possible in regionalizing the use of the gadget, the use of the piece of equipment, or making it available nationwide through electronic means so that we use our moneys as wisely as possible. This will require that we develop a plan and a design for how we work together in this network.

Fifth, we must plan for and create regional computer labs that permit us to share the best expertise and equipment in searching computers. This involves not just cybercrime; it involves drug records, financial data, e-mail by co-conspirators. All this evidence is getting stored on laptops and palm pilots rather than filing cabinets. Sometimes the records to be seized won't be at the search site at all but at a remote server in a commercial network.

Here in California, the shortage of computer forensic experts in Southern California lead to the creation of the first regional computer forensic lab, which involves the participation of federal, state and local computer forensic examiners. This lab was created through a joint initiative with federal, state and local officials, and it is staffed by 16 computer forensic examiners. I believe that this lab is a model that could be replicated in other jurisdictions.

But, again, we must plan. Where should it go? Let's not compete. Let us work together to make sure we serve this nation as a whole. And let us in the process come together and agree on forensic standards which will be the standards applicable throughout the country, wherever possible, for the admission of evidence seized from computers.

Seventh, I think it is important that we explore potential legal solutions. We should explore new and more robust procedural tools to allow state authorities to more easily gather information located outside their jurisdictional boundaries.

I suggest to you that it is time to open a dialogue on whether a new interstate compact should be crafted which respects each state's autonomy, but that commits each signatory state to honoring and enforcing out-of-state subpoenas, search warrants and traffic trace orders.

If cybercrime finds borders meaningless, we're going to have to be prepared to maintain the autonomy of our states, while at the same time developing processes that permit enforcement against those that would ignore boundaries. For example, if Ohio prosecutors need to issue an investigative subpoena for records of a fraudulent website located in Georgia, there is currently no formal procedural mechanism to ensure the enforcement of that out-of-state subpoena.

We need to develop an enforceable legal process. We should also consider possible legislative solutions. One example would be a state law requiring service providers to accept service of process and comply with out-of-state subpoenas, court orders and search warrants. I understand that California has adopted legislation in this area, and I encourage you to consider whether it would be helpful in your state.

And finally, we would appreciate your thoughts as to whether there is any federal role consistent with principles of federalism and state sovereignty. Would it assist you, for example,

if a federal statute allowed states to apply to federal courts for orders with national application.

These are the issues that I think we need to discuss as part of a network in developing answers to enable us to address cybercrime in the most effective manner possible. I have been speaking of a cooperative network based in this country. But we must look beyond. International borders don't mean anything either. And that is the reason we have reached out to the other ministers of justice, to police authorities in the big industrial nations, the eight big industrial nations of the world, to form a cyber partnership. We have a 24-hour, seven-day-a-week response time in most of these nations now, and it is working. But we have got to do something to move our efforts ahead.

The Office of International Affairs in the Department of Justice has tried to be available to work with you, but the whole concept of the globalization of crime because of the Internet is making their work more and more critical, and they are becoming spread thin.

We must develop means of supporting them so that we can support you with one common goal. The cyber criminal should get the clear message that there is no safe place to hide in this world, and you can't hide just because you are halfway around the world from where the crime was

felt here in the United States. We must improve the extradition processes that permit the extradition of nationals -- and I look forward to working with you in that area -- and we must make sure that people understand there is going to be a consequence for a hacking, a consequence for a cyber stalking, a consequence for a terrorist threat.

And some people will say that, how are we going to afford to bring them all the way around the world for trial? We're going to have to look for new and innovative means of enforcing the law.

And one of the things I think we should explore is the development of video conferencing in which a number of states, I believe, have participated. I know of at least one that permits testimony in another country to be had in the courtroom here through video conferencing.

Right now we must act. People must know that they can not make idle threats across the Internet that terrify students at Columbine High. They must know that there will be consequences for their act. And I believe this network can do much to advance that. The next issue -- and Christine said she liked this topic a lot -- is dollars. Fighting crime on the Internet is and will continue to be an expensive endeavor.

As a former state prosecutor, I am well aware of the great strains on the budgets of state and local law enforcement. Sharing our expertise and cooperation in research and development will help to avoid unnecessary expensive duplication. But the cost of developing and updating technical investigative and prosecutorial expertise and technology will require more than simply sharing the burden.

We must work with our county counsels, state legislatures and Congress to help them understand the importance of this effort, and to help them create a reasonable plan for the nation to provide resources in the most reasoned way possible to fight this effort.

We are working through our office of justice programs to do everything we can, along with the FBI, to be a good partner in dollars as well, but we have a long way to go. An issue of great importance to me is our ninth step that I think we must consider, and that is the issue of privacy. Privacy advocates don't trust us very much. Industry sometimes doesn't trust us very much. And we are going to have to do something about it.

We're going to have to do some outreach, begin some meetings, and let people know that we're all concerned about privacy issues. And nobody likes to pick up the New York Times and see extortion on the front page of the New York Times. Neither the privacy advocate nor the law enforcement person. And we all want one principal goal, and that is that it not happen in the first place. And if we can't avoid that, we want to make sure that that person is held accountable.

We have to make industry and privacy experts understand that no one wants to allow the invasion of people's privacy. We have to work with them to make sure that the Constitution is upheld; that it is, indeed, a living document; that it is capable of being applied to technology that Alexander Hamilton and James Madison never ever dreamed of.

And finally, I think we can play an important role with our colleagues in education in helping educate our populace, and particularly our children, about the ethical responsibilities of using this powerful tool.

It was first brought to mind when I met with representatives of the telecommunications industries. One leader said, "You know, you've made me think. My 13-year-old daughter knows that she should not steal, that she should not read other people's mail, that she shouldn't go into their bedroom when they're not there and poke around, but I don't think she knows what she should and shouldn't do on the Internet." As part of this network, I think we could be a powerful force in shaping ethical considerations and teaching ethical responsibilities on the net.

As I said at the outset, you all are some of the great public servants that I have worked with. I admire your dedication, your absolute commitment and persistence. I firmly believe that the issues you all discuss at this conference will shape the future of law enforcement indefinitely.

As you confront this challenge, I want you to know that the Justice Department wants to work with you in every way we possibly can as an equal, respectful partner.

I know you have other ideas that come from your firsthand experience with these issues, and I would love to hear them. I'd like to invite you to come to Washington as soon as possible to begin work if you are willing to formally establish this (inaudible due to loud cough from audience).

Our response or our failure to respond, either in this fashion or some other, to these challenges today will determine our ability to fight crime for many tomorrows to come. We can only do this together. We have shown what we can together. Let's get started now.



**THE ELECTRONIC FRONTIER: THE CHALLENGE OF  
UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET**  
A Report of the President's Working Group  
on Unlawful Conduct on the Internet

March 2000

---

**TABLE OF CONTENTS**

**EXECUTIVE SUMMARY**

**I. INTRODUCTION**

- A. Executive Order
- B. The Working Group on Unlawful Conduct on the Internet
- C. Summary of Strategy

**II. POLICY FRAMEWORK AND LEGAL ANALYSIS**

A. Understanding the Nature of Unlawful Conduct Involving Computers

- 1. Computers as Targets
- 2. Computers as Storage Devices
- 3. Computers as Communications Tools

B. A Framework for Evaluating Unlawful Conduct on the Internet

- 1. Online-Offline Consistency
- 2. Appropriate Investigatory Tools
- 3. Technology-Neutrality
- 4. Consideration of Other Societal Interests

C. Promoting Private Sector Leadership

D. Sufficiency of Existing Federal Laws

- 1. Analysis of Substantive Laws
- 2. New Investigatory Challenges

### III. LAW ENFORCEMENT NEEDS AND CHALLENGES

#### A. Protecting Computers and Networks

#### B. Federal Tools and Capabilities

1. Personnel, Equipment, and Training
2. Locating and Identifying Cybercriminals
3. Collecting Evidence

#### C. State and Local Tools and Capabilities

1. Jurisdiction
2. Interstate and Federal-State Cooperation
3. Resources

#### D. Legal Authorities: Gaps in Domestic Laws

1. Pen Register and Trap and Trace Statute
2. Computer Fraud and Abuse Act
3. Privacy Protection Act
4. Electronic Communications Privacy Act
5. Telephone Harassment
6. Cable Communications Policy Act

#### E. Challenges for International Cooperation

1. Substantive International Criminal Law
2. Multilateral Efforts
3. Continuing Need for International Cooperation

### IV. THE ROLE OF PUBLIC EDUCATION AND EMPOWERMENT

#### A. Educating and Empowering Parents, Teachers, and Children

1. Technological Tools
2. Non-technological Tools

#### B. Educating and Empowering Consumers

1. FTC Initiatives: Using Technology to Educate Consumers
2. Department of Commerce Initiatives
3. FDA's Outreach Campaign
4. SEC's Investor Education Efforts
5. CPSC's Consumer Outreach Efforts

#### C. Developing Cyberecitizens

### V. CONCLUSIONS AND RECOMMENDATIONS

## APPENDICES

A EXECUTIVE ORDER 13,133

B INTERNET FRAUD

C ONLINE CHILD PORNOGRAPHY

D INTERNET SALE OF PRESCRIPTION DRUGS AND CONTROLLED SUBSTANCES

E INTERNET SALE OF FIREARMS

F INTERNET GAMBLING

G INTERNET SALE OF ALCOHOL

H ONLINE SECURITIES FRAUD

I SOFTWARE PIRACY AND INTELLECTUAL PROPERTY THEFT

J MULTILATERAL EFFORTS

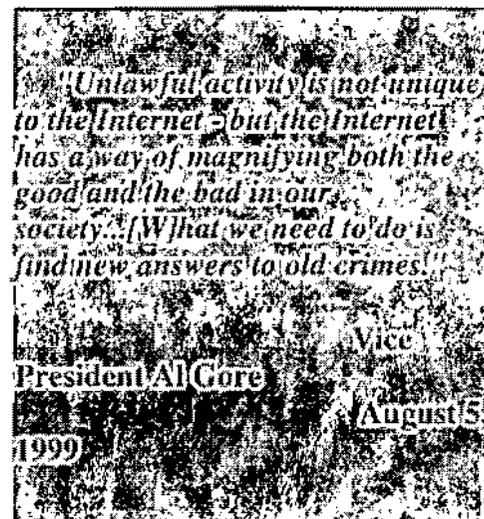
---

**THE ELECTRONIC FRONTIER: THE CHALLENGE OF  
UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET**  
A Report of the President's Working Group  
on Unlawful Conduct on the Internet  
March 2000

### EXECUTIVE SUMMARY

The Internet is rapidly transforming the way we communicate, educate, and buy and sell goods and services. As the Internet's potential to provide unparalleled benefits to society continues to expand, however, there has been an increasing recognition that the Internet can also serve as a powerful new medium for those who wish to commit unlawful acts has also grown.

Unlawful conduct involving the use of the Internet is just as intolerable as any other type of illegal activity. Ensuring the safety and security of those who use the Internet is thus a critical element of the Administration's overall policy regarding the Internet and electronic commerce, a policy that seeks to promote private sector leadership, technology-neutral laws and regulation, and an appreciation of the Internet as an important medium for commerce and communication both domestically and internationally. Indeed, the continued growth and maturation of this new medium depends on our taking a balanced approach that ensures that the Internet does not become a haven for unlawful activity.



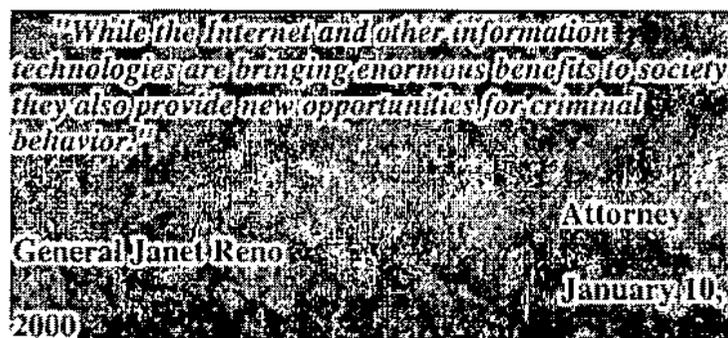
For these reasons, the President and Vice President established an interagency Working Group on Unlawful Conduct on the Internet, chaired by the Attorney General, to provide an initial analysis of legal and policy issues surrounding the use of the Internet to commit unlawful acts. Specifically, the Working Group considered (1) the extent to which existing

federal laws are sufficient to address unlawful conduct involving the use of the Internet; (2) the extent to which new tools, capabilities, or legal authorities may be needed for effective investigation and prosecution of such conduct; and (3) the potential for using education and empowerment tools to minimize the risks from such conduct.

Consistent with the Administration's overall policy, the Working Group recommends a 3-part approach for addressing unlawful conduct on the Internet:

- *First*, any regulation of unlawful conduct involving the use of the Internet should be analyzed through a policy framework that ensures that online conduct is treated in a manner consistent with the way offline conduct is treated, in a technology-neutral manner, and in a manner that takes account of other important societal interests, such as privacy and protection of civil liberties;
- *Second*, law enforcement needs and challenges posed by the Internet should be recognized as significant, particularly in the areas of resources, training, and the need for new investigative tools and capabilities, coordination with and among federal, state, and local law enforcement agencies, and coordination with and among our international counterparts; and
- *Third*, there should be continued support for private sector leadership and the development of methods – such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts – that educate and empower Internet users to prevent and minimize the risks of unlawful activity.

Prior technological advances – the automobile, the telegraph, and the telephone, for example – have brought dramatic improvements for society, but have also created new opportunities for wrongdoing. The same is true of the Internet, which provides unparalleled opportunities for socially beneficial endeavors – such as education, research, commerce, entertainment, and discourse on public affairs – in ways that we may not now even be able to imagine. By the same token, however, individuals who wish to use a computer as a tool to facilitate unlawful activity may find that the Internet provides a vast, inexpensive, and potentially anonymous way to commit unlawful acts, such as fraud, the sale or distribution of child pornography, the sale of guns or drugs or other regulated substances without regulatory protections, and the unlawful distribution of computer software or other creative material protected by intellectual property rights.



In its analysis of existing federal laws in these and other areas, the Working Group finds that existing substantive federal laws generally do not distinguish between unlawful conduct

committed through the use of the Internet and the same conduct committed through the use of other, more traditional means of communication. For example, laws governing fraud – such as credit card fraud, identity theft, securities fraud, gambling, and unfair and deceptive trade acts or practices – apply with equal force to both online as well as offline conduct. To the extent these existing laws adequately address unlawful conduct in the offline world, they should, for the most part, adequately cover unlawful conduct on the Internet. There may be a few instances, however, where relevant federal laws need to be amended to better reflect the realities of new technologies, such as the Internet.

Despite the general adequacy of laws that define the substance of criminal and other offenses, the Working Group finds that the Internet presents new and significant investigatory challenges for law enforcement at all levels. These challenges include: the need for real-time tracing of Internet communications across traditional jurisdictional boundaries, both domestically and internationally; the need to track down sophisticated users who commit unlawful acts on the Internet while hiding their identities; the need for hand-in-glove coordination among various law enforcement agencies; and the need for trained and well-equipped personnel – at federal, state, local, and global levels – to gather evidence, investigate, and prosecute these cases. In some instances, federal procedural and evidentiary laws may need to be amended to better enable law enforcement to meet these challenges.

These needs and challenges are neither trivial nor theoretical. Law enforcement agencies today, for example, are faced with the need to evaluate and to determine the source, typically on very short notice, of anonymous e-mails that contain bomb threats against a given building or threats to cause serious bodily injury. Other scenarios raise similarly significant concerns: If a hacker uses the Internet to weave communications through computers in six different countries to break into an online business' records of customer credit card information, consumer confidence in the security of e-commerce and the Internet may be damaged if law enforcement agencies are unable to cooperate and coordinate rapidly with their counterparts in the other countries to find the perpetrator.

Finally, an essential component of the Working Group's strategy is continued support for private sector leadership and the development of methods – such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts – that educate and empower Internet users so as to minimize the risks of unlawful activity. This Administration has already initiated numerous efforts to educate consumers, parents, teachers, and children about ways to ensure safe and enjoyable Internet experiences, and those efforts should continue. The private sector has also undertaken substantial self-regulatory efforts – such as voluntary codes of conduct and appropriate cooperation with law enforcement – that show responsible leadership in preventing and minimizing the risks of unlawful conduct on the Internet. Those efforts must also continue to grow. Working together, we can ensure that the Internet and its benefits will continue to grow and flourish in the years and decades to come.

**THE ELECTRONIC FRONTIER: THE CHALLENGE OF  
UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET**  
A Report of the President's Working Group  
on Unlawful Conduct on the Internet  
March 2000

*On April 7, 1999, visitors to an online financial news message board operated by Yahoo!, Inc. got a scoop on PairGain, a telecommunications company based in Tustin, California. An e-mail posted on the message board under the subject line "Buyout News" said that PairGain was being taken over by an Israeli company. The e-mail also provided a link to what appeared to be a website of Bloomberg News Service, containing a detailed story on the takeover. As news of the takeover spread, the company's publicly traded stock shot up more than 30 percent, and the trading volume grew to nearly seven times its norm. There was only one problem: the story was false, and the website on which it appeared was not Bloomberg's site, but a counterfeit site. When news of the hoax spread, the price of the stock dropped sharply, causing significant financial losses to many investors who purchased the stock at artificially inflated prices.*

*Within a week after this hoax appeared, the Federal Bureau of Investigation arrested a Raleigh, North Carolina man for what was believed to be the first stock manipulation scheme perpetrated by a fraudulent Internet site. The perpetrator was traced through an Internet Protocol address that he used, and he was charged with securities fraud for disseminating false information about a publicly traded stock. The Securities and Exchange Commission also brought a parallel civil enforcement action against him. In August, he was sentenced to five years of probation, five months of home detention, and over \$93,000 in restitution to the victims of his fraud.*

## I. INTRODUCTION

The use of new technology to commit traditional crimes, such as securities fraud, is not new. Advances in technology – the advent of the automobile and the telephone, for instance – have always given wrongdoers new means for engaging in unlawful conduct. The Internet is no different: it is simply a new medium through which traditional crimes can now be committed, albeit through the use of inexpensive and widely available computer and telecommunications systems, and with unprecedented speed and on a far-reaching scale. At the same time, as exemplified by the PairGain case, the tools and capabilities associated with new technologies can in many instances help law enforcement agencies solve such crimes.

How should society, and government in particular, respond to the advent of these new ways of committing traditional crimes? This report responds to a recent Executive Order from the President and sketches the preliminary contours of a legal and policy answer to that question. It provides a foundation and offers a framework for further dialogue among law enforcement officials and policymakers at all levels; members of the business community, trade associations, and the non-profit sector; and members of the public on one of the most important issues we face in response to this powerful new communications medium and our new digital economy.

### A. Executive Order 13,133

In August 1999, President Clinton established an interagency Working Group on Unlawful Conduct on the Internet ("Working Group"). Executive Order 13,133 directed the Working Group, under the leadership of the Attorney General, to address the issue of unlawful conduct

involving the use of the Internet and to prepare a report with recommendations on:

- 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 sale of guns, explosives, controlled substances, and prescription drugs, as well as fraud and child pornography;
- 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
- 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.

The Executive Order further directed the Working Group to conduct its review in the context of current Administration policy concerning the Internet. That policy includes support for industry self-regulation where possible, support for technology-neutral laws and regulations, and an appreciation of the Internet as an important medium for commerce and free speech both domestically and internationally.<sup>1</sup> The full text of the Executive Order appears in Appendix A to this report.

This report responds to the directive of Executive Order 13,133 and sets forth a strategy for responding to unlawful conduct on the Internet and for ensuring a safe and secure online environment. As discussed in greater detail below, the Working Group's proposed strategy consists of a 3-part approach that includes: (a) a framework of policy principles for evaluating the need for Internet-specific laws to prohibit unlawful conduct; (b) recognition of the new and significant investigatory needs and challenges posed by the Internet; and (c) support for private sector leadership and the development of appropriate technological tools and outreach efforts to educate and empower Internet users to prevent and minimize the risks of unlawful acts facilitated by the Internet.

Part II of this report focuses on the first component of the strategy, describing the nature of unlawful activity on the Internet and proposing a framework for analyzing policy and legal responses to such activity. Part II also discusses efforts to promote private-sector leadership in this area and summarizes the Working Group's analysis of the adequacy of existing substantive federal laws, as applied to unlawful conduct on the Internet. Part III of the report then identifies several areas in which new technology tools, capabilities, or legal authorities may be required for effective evidence-gathering, investigation, and prosecution of unlawful conduct that involves the use of the Internet. Part IV of the report focuses on the third component of the strategy, urging support for expanded educational efforts and technological tools to empower Internet users. Finally, Part V summarizes the report's conclusions and recommendations for further action.

## **B. The Working Group on Unlawful Conduct on the Internet**

Pursuant to Executive Order 13,133, the Working Group included the Attorney General, who served as chair of the Working Group; the Director of the Office of Management and Budget; the Secretary of the Treasury; the Secretary of Commerce; the Secretary of Education; the Director of the Federal Bureau of Investigation; the Director of the Bureau of Alcohol,

Tobacco and Firearms; the Administrator of the Drug Enforcement Administration; the Chair of the Federal Trade Commission; and the Commissioner of the Food and Drug Administration. In addition, given their interest and expertise in the subject matter, representatives from the Consumer Product Safety Commission, the U.S. Customs Service, the Department of Defense, the Department of State, the National Aeronautics and Space Administration, the National Commission on Libraries and Information Science, the Postal Inspection Service, the U.S. Secret Service, and the Securities and Exchange Commission also participated on the Working Group.

In preparing this report, the Working Group benefitted from the views of representatives of a variety of entities outside the federal government, including, for example:

- State and local groups, such as the National Association of Attorneys General; the National District Attorneys Association; the National Association of Boards of Pharmacies; and the National League of Cities;
- Industry groups, such as the Internet Alliance, the Computer Systems Policy Project, the Business Software Alliance, and representatives of Internet service providers and other high-technology companies; and
- Non-profit advocacy and civil liberties groups, such as the National Center for Missing and Exploited Children, the Center for Democracy and Technology, and the Electronic Privacy Information Center.

We look forward to continuing our dialogue with these and other groups on the important and substantial issues raised in this report.

### C. Summary of Strategy

The Internet already is and will continue to be a major force for communication and economic growth in the decades ahead. Consistent with its 1997 *Framework for Global Economic Commerce*, the Administration is continuing to work toward providing a market-oriented policy environment to support the development of this new digital economy. In developing such an environment, it is essential to address some of the possible negative side effects associated with this new economy. These goals are not inconsistent: rather, they are mutually reinforcing: continued growth in economic commerce will require a stable, predictable legal environment that includes vigorous enforcement of consumer protections; and focused law enforcement efforts in turn will promote greater consumer confidence and trust in the Internet as a safe and secure medium of communications and commerce.

To further these goals, the Working Group recommends a 3-part approach for addressing unlawful conduct on the Internet:

- *First*, evaluating the need for Internet-specific regulation of unlawful conduct through a framework of general policy principles, including the principle that online and offline conduct should be treated consistently and in a technology-neutral way;
- *Second*, recognizing the significant law enforcement needs and challenges posed by the Internet, particularly in the areas of resources, training, and the need for

new investigatory tools and capabilities, coordination with and among federal, state, and local law enforcement agencies, and coordination with and among our international counterparts; and

• *Third*, supporting continued private sector leadership and the development of methods – such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts – that educate and empower Internet users so as to prevent and minimize the risks of unlawful activity.

Each of these components is an integral part of our overall proposed strategy and is discussed in greater detail in the report that follows.

## II. POLICY FRAMEWORK AND LEGAL ANALYSIS

There can be little doubt that the Internet – a global electronic network of computer networks (including the World Wide Web) that connects people and information <sup>2</sup> – has revolutionized and will continue to revolutionize how we communicate, educate ourselves, and buy and sell goods and services. The Internet has grown from 65 million users in 1998 to over 100 million users in the U.S. in 1999, or half the country's adult population; the number of Internet users in the U.S. is projected to reach 177 million by the end of 2003; and the number of Internet users worldwide is estimated to reach 502 million by 2003. <sup>3</sup> Business-to-business electronic commerce totaled over \$100 billion in 1999 (more than doubling from 1998) and is expected to grow to over \$1 trillion by 2003. <sup>4</sup>

There can also be little doubt that the Internet provides immeasurable opportunities for far-reaching social benefits. Communications over the Internet, for example, permits unparalleled opportunities for education, research, commerce, entertainment, and discourse on public affairs. Electronic mail ("e-mail") has become an entirely new medium for business and personal communications, allowing users a fast and inexpensive way to keep in touch, to send text, pictures, or sound files to individuals or to groups, and to buy and sell goods and services. News and other information can be made available to anyone with a computer and a modem virtually instantaneously, and more information (on an absolute scale) can be made available to more people, due to the open and decentralized nature of the Internet (anyone can put up a website and "publish" information for the world to see). Access to research databases, directories, encyclopedias, and other information sources previously available only to those with the time, money, and energy to obtain physical access to print material has opened up a world of information to the average citizen. And by making transactions of all kinds cheaper, faster, interactive, and hence more efficient, electronic commerce ("e-commerce") is transforming the way businesses operate and the way consumers work, shop, and play.

The Internet, like most new technologies, is an inherently value-neutral tool: It can be used in ways that are socially beneficial or socially harmful. New technologies can, of course, create new forms of socially undesirable behavior. More often, they provide new ways of committing traditionally undesirable behavior. For example, the advent of the telephone allowed innovative lawbreakers not only to develop new crimes (e.g., long-distance toll fraud), but also to commit traditional crimes in a new manner (e.g., harassment through the use of the telephone).

The Internet has fared no better than other technologies against resourceful and technologically sophisticated individuals who seek to commit unlawful acts. Last year, for

example, tens of thousands of computer users were struck by "Melissa" and "Explore.Zip.Worm," e-mail viruses that quickly spread around the world, erasing files, crashing systems, and costing companies millions of dollars in support and downtime. More recently, some of the most popular consumer and commercial websites were temporarily disabled as a result of "distributed denial-of-service" attacks. Other websites have been the targets of "page-jacking" schemes, in which websites and search engines are manipulated to drive unsuspecting users to unwanted (usually "adult") websites (see Appendix B for further discussion of page-jacking).

More generally, individuals who wish to use a computer as a tool to facilitate criminal activity may find the Internet as appealing, if not more so, as they did the telephone decades ago or the telegraph before that. Similar to the technologies that have preceded it, the Internet provides a new tool for wrongdoers to commit crimes, such as fraud, the sale or distribution of child pornography, the sale of guns or drugs or other regulated substances without regulatory protections, or the unlawful distribution of computer software or other creative material protected by intellectual property rights. In the most extreme circumstances, cyberstalking and other criminal conduct involving the Internet can lead to physical violence, abductions, and molestation. Although the precise extent of unlawful conduct involving the use of computers is unclear, 5 the rapid growth of the Internet and e-commerce has made such unlawful conduct a critical priority for legislators, policymakers, industry, and law enforcement agencies.

#### **A. Understanding the Nature of Unlawful Conduct Involving Computers**

Although definitions of computer crime may differ, not every crime committed with a computer is a computer crime. For example, if someone steals a telephone access code and makes a long distance call, the code they have stolen is checked by a computer before the call is processed. Even so, such a case is more appropriately treated as "toll fraud," not computer crime. Although this example may seem straightforward, many cases cannot be so neatly categorized. For example, a bank teller who steals a \$10 bill from a cash drawer is embezzling. A bank teller who writes a computer program to steal pennies from many accounts (at random) and to funnel that money into another bank through the electronic funds transfer system may also be embezzling, but both committing and prosecuting this offense may require a working knowledge of the bank's computer system. Thus, such a crime may reasonably be characterized as a computer offense.

Broadly speaking, computers can play three distinct roles in a criminal case. First, a computer can be the target of an offense. This occurs when conduct is designed to take information without authorization from, or cause damage to, a computer or computer network. The "Melissa" and "Explore.Zip.Worm" viruses, along with "hacks" into the White House and other websites, are examples of this type of offense. Second, a computer can be incidental to an offense, but still significant for law enforcement purposes. For example, drug traffickers may store transactional data (such as names, dates, and amounts) on computers, rather than in paper form. Third, computers can be a tool for committing an offense, such as fraud or the unlawful sale of prescription drugs over the Internet. Each of these three roles can be and often are present in a single criminal case. Although this report focuses primarily on this third category of computer crime, it is important to understand the range of unlawful conduct that involves computers to appreciate the context of law enforcement needs and challenges relating to such conduct.

##### **1. Computers as Targets**

One obvious way in which a computer can be involved in unlawful conduct is when the confidentiality, integrity, or availability of a computer's information or services is attacked. This form of crime targets a computer system, generally to acquire information stored on that computer system, to control the target system without authorization or payment (theft of service), or to alter the integrity of data or interfere with the availability of the computer or server. Many of these violations involve gaining unauthorized access to the target system (i.e., "hacking" into it).

Offenses involving theft of information may take a variety of forms, depending on the nature of the system attacked. Sensitive information stored on law enforcement and military computers offers a tempting target to many parties, including subjects of criminal investigations, terrorist organizations, and foreign intelligence operatives.

Hackers also target non-governmental systems to obtain proprietary or other valuable information. For example, a hacker might gain access to a hotel reservation system to steal credit card numbers. Other cases may fall into the broad category of intellectual property theft. This includes not only the theft of trade secrets, but also much more common offenses involving the unauthorized duplication of copyrighted materials, especially software programs. Other cases may involve a perpetrator who seeks private information about another individual, whether as a means to an end (e.g., to extort money or to embarrass the victim through public disclosure), to obtain a commercial advantage, or simply to satisfy personal curiosity. Targets in this category include systems containing medical records, telephone customer records (such as call records or unlisted directory information), or consumer credit report information.

Computers can also be the target of an offense in cases where an offender gains unauthorized access to a system. For instance, an offender may use his computer to break into a telephone switching system (including a private system, such as a PBX) to steal long-distance calling services. (This type of telephone equipment manipulation is often referred to as "phone phreaking" or simply "phreaking.") In some cases, hackers have used the resources of compromised systems to perform intensive computational tasks such as cracking encrypted passwords stolen from other sites. The theft-of-service offenses are often associated with the practice of "weaving," in which a hacker traverses multiple systems (and possibly multiple telecommunications networks, such as the Internet or cellular and landline telephone networks) to conceal his true identity and location. In this scenario, the sole reason for breaking into a given computer may be to use it as a stepping-stone for attacks on other systems.

A more insidious type of damage takes place in cases where the attacker compromises a system in furtherance of a larger scheme. The most well-known examples of this type of attack have involved telephone network computers. In one case, a hacker manipulated telephone switching equipment to guarantee that he would be the winning caller in several call-in contests held by local radio stations. The fruits of his scheme included two sports cars and \$30,000 in cash. Internet-connected computers are subject to similar types of attacks. Routers – which are computers that direct data packets traveling on the Internet – are analogous to telephone switches and thus are tempting targets for skilled hackers who are interested in disrupting, or even rerouting, communications traffic on the network.

In the category of attacks known collectively as "denial of service," the objective is to disable

the target system without necessarily gaining access to it. One technically straightforward method of accomplishing this objective is "mailbombing," the practice of sending large volumes of e-mail to a single site (or user account) to clog the mail server or even to cause the target host to crash. Other methods – ranging from simply tying up incoming phone lines to more sophisticated attacks using low-level data transmission protocols – may also be used to achieve the same end: rendering the target system unavailable for normal use. These sorts of denial-of-service attacks recently received much publicity when several major websites, including Yahoo.com, Amazon.com, eBay.com, and Buy.com, were temporarily disabled as a result of such attacks.

## 2. Computers as Storage Devices

A second way in which computers can be used to further unlawful activity involves the use of a computer or a computer device as a passive storage medium. As noted above, drug dealers might use computers to store information regarding their sales and customers. Another example is a hacker who uses a computer to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or "warez" (pirated commercial software). As discussed in Part III below, computers often can provide valuable evidence that may help law enforcement respond to unlawful conduct.

Indeed, computers have made it possible for law enforcement agencies to gather some information that may not have been previously even maintained in the physical world. For example, an unsophisticated offender, even after "deleting" computer files (as opposed to destroying paper records), might leave evidence of unlawful activity that a trained computer forensic expert could recover. In addition, because an average computer with several gigabytes of memory can contain millions of pages of information, a law enforcement agent might, pursuant to lawful authority (such as a warrant), find volumes of information in one place. Of course, that information is only useful if there are trained computer experts on hand in a timely fashion, familiar with the relevant computer hardware or software configuration, to search the computer for specific information and to retrieve it in readable form (see generally Part III.B below).

## 3. Computers as Communications Tools

Another way that a computer can be used in a cybercrime is as a communications tool. Many of the crimes falling within this category are simply traditional crimes that are committed online. Indeed, many of the examples in this report deal with unlawful conduct that exists in the physical, "offline" world – the illegal sale of prescription drugs, controlled substances, alcohol, and guns; fraud; gambling; and child pornography. These examples are, of course, only illustrative; online facilities may be used in the furtherance of a broad range of traditional unlawful activity. E-mail and chat sessions, for example, can be used to plan or coordinate almost any type of unlawful act, or even to communicate threats or extortion demands to victims (see cyberstalking box).

### Cyberstalking

Cyberstalking is a prime example of the use of computers and the Internet to facilitate a traditional offline crime. Cyberstalking generally refers to the use of the Internet, e-mail, or other electronic communications devices to "stalk" another person — where "stalking" in the traditional sense means to engage in repeated harassing or threatening behavior (such as following a person, appearing at a person's home or workplace, making harassing telephone calls, or leaving written messages or objects) that places the victim in reasonable fear of death or bodily injury, cf. 18 U.S.C. § 2261A (prohibiting interstate stalking).

The Internet provides new avenues for would-be stalkers to pursue their victims. For example, in April 1999, a 50-year-old former security guard pled guilty (under California law) to one count of stalking and three counts of solicitation of sexual assault for using the Internet to solicit the rape of a woman who rejected his romantic advances. The defendant impersonated the victim in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized about being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the victim's door, saying they wanted to rape her. The defendant faces up to six years in prison.

In August 1999, in response to a request from the Vice President, the Attorney General issued a report, *Cyberstalking: A New Challenge for Law Enforcement and Industry* (available at [www.usdoj.gov/criminal/cybercrime/](http://www.usdoj.gov/criminal/cybercrime/)), exploring the nature of cyberstalking, analyzing the adequacy of current federal and state laws, and recommending ways to improve efforts against cyberstalking. The conclusions of that report track the primary conclusions of this report — although existing laws (in most instances) may cover the unlawful conduct at issue, the use of the Internet presents numerous investigatory challenges (e.g., those relating to jurisdiction and anonymity) that need to be addressed. The report also found that industry must continue to take an active role in educating and protecting online users against Internet-facilitated unlawful conduct.

Just as legitimate use of the Internet is growing, so too is the Internet increasingly being used to facilitate traditional offenses. For example, because e-mail allows private communications between parties, individuals have used the Internet to send threatening e-mails (including threats to the President). The Internet's one-to-many broadcast capability has also allowed individuals to falsely advertise goods on the Internet or on a website.

The Internet's file transfer capability also enables the Internet to be used as a product delivery system. Because large files can be copied and transmitted reliably, quickly, and cheaply, software companies are now selling software over the Internet: the buyer simply provides a credit card number and downloads the software from the Internet to his or her personal computer. This same capability unfortunately allows for the unauthorized reproduction and distribution of copyrighted software.

Some criminal activities employ both the product delivery and communications features of the Internet. For example, pedophiles may use the Internet's file transfer utilities to distribute and receive child pornography, and use its communications features to make contact with children. Because users need not transmit their voice or appearance, it is easy for an adult to pose as a child and to gain the confidence of children online.

As noted above, this report's primary focus is on this third way in which computers can be used to commit unlawful acts — the use of computers and modern telecommunications facilities as tools (analogous to the use of telephones as tools) to commit an offense. Many of the enforcement and investigative challenges associated with unlawful conduct on the Internet,

however, extend to all three ways in which computers can be used for unlawful activity. Consequently, the recommendations contained in this report, if acted upon, could assist law enforcement agencies in combating all types of unlawful conduct involving the use of the Internet.

## **B. A Framework for Evaluating Unlawful Conduct on the Internet**

In its assessment of the extent to which existing federal laws are sufficient to address unlawful conduct involving the use of the Internet, the Working Group developed four general principles to guide its analysis. These principles form the basis for the analytical framework proposed by the Working Group for evaluating the need, if any, for Internet-specific regulation of the particular conduct at issue. The principles flow from the Administration's overall pursuit of policies that recognize and support the enormous potential economic and social benefits of the medium, without unintentionally stifling its growth.

### 1. Online-Offline Consistency

First, substantive regulation of unlawful conduct (e.g., legislation providing for civil or criminal penalties for given conduct) should, as a rule, apply in the same way to conduct in the cyberworld as it does to conduct in the physical world. If an activity is prohibited in the physical world but not on the Internet, then the Internet becomes a safe haven for that unlawful activity. Similarly, conduct that is not prohibited in the physical world should not be subject to prohibition merely because it is carried out in cyberspace.

Thus, the first step in any analysis of unlawful conduct involving the use of the Internet is to examine how the law treats the same conduct in the offline world. That is, unlawful conduct involving the use of the Internet should not be treated as a special form of conduct outside the scope of existing laws. For example, fraud that is perpetrated through the use of the Internet should not be treated any differently, as a matter of substantive criminal law, from fraud that is perpetrated through the use of the telephone or the mail. To the extent existing laws treat online and offline conduct inconsistently, they should be amended to remove inconsistencies. ¶ As the discussion below and the detailed analyses of several examples in the appendices to this report illustrate, however, existing substantive law is generally sufficient to cover unlawful conduct involving the use of the Internet.

### 2. Appropriate Investigatory Tools

Second, to enforce substantive laws that apply to online conduct, law enforcement authorities need appropriate tools for detecting and investigating unlawful conduct involving the Internet. For example, as discussed in greater detail below, to the extent existing investigative authority is tied to a particular technology, it may need to be modified or clarified so that it also applies to the Internet.

Indeed, new technologies may justify new forms of investigative authority. Before the invention of the telephone, for example, law enforcement had no need for wiretaps, but once it was clear that the telephone was being used to facilitate illegal activity, that new authority – circumscribed with protections for civil liberties and other societal interests – became necessary and appropriate. Similarly, features of the Internet that make it different from prior technologies may justify the need for changes in laws and procedures that govern the detection and investigation of computer crimes. These features, highlighted here in summary form, are

discussed in greater detail below:

- *The global and boundaryless nature of the Internet* means that different law enforcement agencies in different jurisdictions will have to cooperate and coordinate their activities in ways that they have probably never before done.
- *Anonymity* on the Internet can provide social benefits, but misrepresentation of identity can also facilitate fraud and deception. Misrepresentation of identity can also result in access by children to inappropriate material and can create law enforcement investigatory challenges, especially if perpetrated by sophisticated computer users, for it can make criminal activity on the Internet more difficult to detect and prove.
- *The potential to reach vast audiences easily* means that the scale of unlawful conduct involving the use of the Internet is often much wider than the same conduct in the offline world. To borrow a military analogy, use of the Internet can be a "force multiplier."
- *The routine storage of information that can be linked to an individual* can often provide more information to law enforcement (where an individual has been identified or a computer lawfully seized) than may be available in the offline world, but only if the electronic information is handled properly by a trained investigator and if the information obtained is ultimately available in useable form.

Thus, apart from ensuring that online and offline behavior is treated consistently as a matter of substantive law, legislators and policymakers should examine whether law enforcement agencies have appropriate tools to detect and investigate unlawful conduct involving the Internet. That is, even if Internet-specific laws are unnecessary to ensure that criminal and civil penalties apply to the use of the Internet to facilitate unlawful conduct, it may be necessary to alter or augment law enforcement's tools and authorities to meet the new investigatory challenges that such unlawful conduct presents.

### 3. Technology-Neutrality

Third, to the extent specific regulation of online activity may be necessary (in view of the consistency principle noted above), any such regulation should be drafted in a technology-neutral way. Regulation tied to a particular technology may quickly become obsolete and require further amendment. In particular, laws written before the widespread use of the Internet may be based on assumptions regarding then-current technologies and thus may need to be clarified or updated to reflect new technological capabilities or realities. For example, regulation of "wire communications" may not account for the fact that communications may now occur through wireless means or by satellite. Technology-specific laws and regulations may also "lock-in" a particular technology, hindering the development of superior technology.

### 4. Consideration of Other Societal Interests

Fourth, any government regulation of conduct involving the use of the Internet requires a careful consideration of different societal interests. In addition to society's strong interests in investigating and prosecuting unlawful conduct, society also has strong interests in promoting free speech, protecting children, protecting reasonable expectations of privacy, providing broad access to public information, and supporting legitimate commerce.

As applied to the Internet, consideration of other societal interests can present difficult issues, in part because the Internet is different in important ways from existing, "traditional" modes of communication. For example, the Internet is a multi-faceted communications medium that allows not only point-to-point transmission between two parties (like the telephone), but also the widespread dissemination of information to a vast audience (like a newspaper). Internet-specific laws and policies that operate by analogy to those designed for telephone communications or the press may not fit the new medium. The Internet also presents new issues relating to online expectations of privacy and confidentiality that may or may not have analogs in the offline world. Accordingly, rules and regulations designed to protect the safety and security of Internet users should be carefully tailored to accomplish their objectives without unintended consequences, such as stifling the growth of the Internet or chilling its use as a free and open communication medium.

Another aspect of the need to consider different societal interests is to appreciate the need for an appropriate balance among the roles of the government (whether federal, state, local, or other) and the role of the private sector in formulating solutions to Internet policy issues. For example, because regulation of the practices of medicine and pharmacy has traditionally been the province of the states, regulation of online pharmacies presents difficult federal-state jurisdictional and coordination issues (see Appendix D). And, as discussed in the next section, given the Administration's support for private-sector leadership and market-based self-regulation regarding e-commerce, there must be ongoing and regular dialogue with interested parties and groups to ensure that government policies do not have unintended consequences.

### **C. Promoting Private Sector Leadership**

Consistent with the Administration's overall e-commerce policy, the private sector has a critical role to play in ensuring a safe and secure online environment. The distributed, networked, and decentralized nature of the Internet now means that the "rules of the road" must be global, flexible, effective, and readily adaptable to technological change. In particular, the private sector must take the lead in areas such as the design of new technologies to protect children online, self-regulatory consumer protection initiatives, and coordination and cooperation with law enforcement authorities.

In response to the marketplace, for example, there are now many technological options for shielding children from inappropriate content. As discussed in more detail in Part IV.A below, these technological developments include filtering and blocking software, outgoing information blocks, filtered Internet browsers and search engines, filtered Internet service providers, time blocking mechanisms and monitoring tools. Similarly, child-friendly websites are now widespread on the Internet. These websites allow parents to limit a child's access to sites beyond the web service designated for the child's use. In July 1999, the private sector launched the "GetNet Wise" initiative, a new easy-to-access online resource for parents to help keep their children safe online. "GetNet Wise" is a resource containing information on Internet safety tips, consumer content filtering products, law enforcement contacts, and a guide to quality educational and age appropriate online content. Although none of these tools can guarantee that a child will be shielded at all times from inappropriate material on the Internet, their use gives parents the ability to restrict a child's use to the resources on the Internet that they may deem appropriate.

In addition, in response to challenges issued by Commerce Secretary Daley, industry has worked with consumer representatives to develop consumer protection practices, codes of conduct for business-to-consumer e-commerce, and alternative, easy-to-use mechanisms for consumer resolution, redress, and enforcement.

- \* For example, the Better Business Bureau's online division, BBBOnline, is working with industry, consumer, and government representatives to develop a voluntary code to provide online merchants with guidelines to implement consumer protections. The code includes guidance on key consumer protections such as disclosure of sale terms, data privacy, dispute resolution mechanisms, and non-deceptive advertising.
- \* Another group, the Electronic Commerce and Consumer Protection Group, whose members include America Online, American Express, AT&T, Dell, IBM, Microsoft, Time Warner, Inc., and Visa, is working with consumer leaders to develop an innovative approach to jurisdiction as it applies to consumer protection in a global electronic marketplace. This group is also developing a voluntary code of conduct. The goal of the group is to formulate concrete approaches to protect consumers and facilitate e-commerce.

These creative efforts are important to developing effective consumer protection in e-commerce, because as e-commerce expands to encompass more international business-to-consumer transactions, the traditional means of protecting consumers solely through national laws will become more difficult.

In addition to specific consumer protection initiatives, the private sector's dedication and support for a secure Internet system is crucial to curbing unlawful conduct on the Internet. Not only must industry continue to develop security policies and safeguards for their networks and systems, but it should also continue its efforts to identify security flaws that threaten the Internet. For example, computer experts from industry and the Computer Emergency Response Team Coordination Center of Carnegie-Mellon University recently warned of a new Internet security threat that wrongdoers could potentially use to place malicious programs on a victim's computer and to gather information that a person volunteers on websites, such as credit card and Social Security numbers.<sup>8</sup> The Partnership for Critical Infrastructure Protection will provide a cross-sectoral forum for the private sector to address a variety of infrastructure assurance issues, including information sharing, development of best practices, promotion of needed R&D, and workforce development. Another example of private sector cooperation in this effort is InfraGard, which is an information sharing and analysis partnership among the FBI, private sector companies, academic institutions, and other federal, state, and local agencies. InfraGard serves to increase the security of the national infrastructure through ongoing exchanges of infrastructure-protection information and through education, outreach, and other awareness efforts.

The private sector also has a key role to play in continuing to coordinate and cooperate with law enforcement authorities as appropriate. Industry trade groups, such as the Internet Alliance and the Information Technology Association of America ("ITAA"), have been working to develop public-private cooperative efforts that will mutually benefit law enforcement, industry, and consumers. The Internet Alliance's Law Enforcement and Security Council has been developing parental control software and educational campaigns, opening channels of communication between industry and law enforcement representatives, and

creating training programs for law enforcement and industry on issues of mutual interest. ITAA, through its Cybercitizen Project (see Part IV.C below), is working with the Department of Justice to develop education campaigns, personnel exchange programs, and a directory of industry contacts.

Although the private sector has taken important steps in the areas of prevention and online security, there is still much that industry can do to ensure that the Internet is a safe and secure environment. For example:

- Industry should continue to develop and embrace initiatives to protect consumers and children online. These may include technological tools (e.g., more sophisticated blocking, filtering, and parental control software) as well as non-technological tools (e.g., educational campaigns). In particular, industry should continue to be involved in education programs that teach younger Internet users about online responsibilities and online citizenship.
- Industry should continue to cooperate with law enforcement agencies as appropriate. This does not mean that industry ought to be a "co-regulator" with government or that industry needs to be an online police officer. But it does mean that industry should be a voluntary, responsible partner in society's fight against crime, educating its employees on how to recognize unlawful conduct on the Internet and what to do if they discover such conduct. It means working with law enforcement agencies to develop reliable and efficient procedures and channels of communication and cooperation for processing law enforcement requests and investigative information. As the "Melissa" virus case demonstrates, industry's involvement and reporting of information is often crucial to the investigation and prosecution of online offenders.
- Industry should carefully balance reasonable expectations of customer privacy with the need to ensure a safe and secure online environment. For example, some industry members may not retain certain system data long enough to permit law enforcement to identify online offenders. This does not mean that data retention policies need to be uniform or mandatory. To the contrary, in evaluating the costs and benefits of data retention – which include a wide variety of considerations, including market needs, protection of consumer privacy, and public safety – industry should simply give appropriate weight to the wider value to itself and to society of retaining certain information that, among other things, may be essential to apprehending a lawbreaker.
- Industry should be encouraged to recognize that meaningful self-regulation is in its interest as well as in the interests of its customers. Information technology security programs (that teach employees about computer ethics, responsible online practices, and security policies), for instance, help protect computer systems from intruders as well as online offenders. Indeed, as we noted at the outset of this report (see Part I.C above), law enforcement and industry share a common mission in reducing unlawful online conduct, for a safe and secure online environment is essential to consumer confidence, which is in turn essential to ensuring that the Internet continues to grow as a medium for communications and commerce.

The Working Group looks forward to continuing to work with the private sector and other interested parties and groups in partnership on these important issues.

#### **D. Sufficiency of Existing Federal Laws**

Private sector leadership is, of course, necessary but not sufficient to address unlawful conduct involving the use of the Internet. Substantive criminal laws represent a societal determination, expressed through our democratic institutions of government, that certain conduct is so harmful or morally unacceptable that reliance on self-regulation or the market to regulate the conduct is inappropriate. There is thus a need to evaluate whether existing substantive laws apply to unlawful conduct that is committed through the use of the Internet.

Toward that end, and in the context of the framework of policy principles discussed above, the Working Group analyzed several examples of unlawful conduct involving the use of the Internet. The examples, as discussed in detail in appendices to this report, include not only those specifically mentioned in Executive Order 13,133, but also those taken from our experience with legislative proposals and from Executive branch agencies that have jurisdiction to respond to these forms of unlawful conduct.

##### I. Analysis of Substantive Laws

The Working Group's analysis reveals that existing substantive federal laws appear to be generally adequate to protect users from unlawful conduct on the Internet. As listed and summarized in Table 1 below, such laws generally do not distinguish between unlawful conduct committed through the use of the Internet and the same conduct committed through the use of other, more traditional means of communication.

For example, laws governing fraud – such as credit card fraud, identity theft, securities fraud, and unfair and deceptive trade acts or practices – apply with equal force to both online as well as offline conduct (see Appendix B). Laws prohibiting the distribution and possession of child pornography and the luring of minors across state lines for unlawful sexual activity have been used with success to prosecute and convict those who use the Internet to distribute such material or to communicate with child victims in violation of statutory prohibitions (see Appendix C). And laws that prohibit the dispensing of prescription drugs without a valid prescription from a licensed medical professional can be applied to online pharmacies that dispense prescription drugs without required regulatory safeguards (see Appendix D).

Laws in other areas – the sale of firearms (Appendix E); interstate transmission of gambling information (Appendix F); sale of alcohol (Appendix G); securities fraud (Appendix H); and theft of intellectual property (Appendix I) – also generally apply to online conduct as well as offline conduct. Although existing federal laws generally prohibit Internet gambling, technological advances make it prudent to update existing federal laws to ensure that they are technology-neutral and prohibit gambling activities that did not exist before the advent of the Internet (see Appendix F). And, in the area of intellectual property protection, current Sentencing Guidelines pertaining to intellectual property crimes should be updated to ensure that law enforcement agencies and prosecutors commit the resources to continue to pursue these cases vigorously (see Appendix I).

#### **Table 1 – Summary of Analysis of Existing Federal Law**

---

Types of Unlawful Conduct	Examples of Potentially Applicable Federal Laws	Detailed Discussion in Appendix
Internet Fraud	15 U.S.C. §§ 45, 52 (unfair or deceptive acts or practices; false advertisements) 15 U.S.C. § 1644 (credit card fraud) 18 U.S.C. §§ 1028, 1029, 1030 (fraud in connection with identification documents and information; fraud in connection with access devices; and fraud in connection with computers) 18 U.S.C. § 1341 et seq. (mail, wire, and bank fraud) 18 U.S.C. § 1345 (injunctions against fraud) 18 U.S.C. § 1956, 1957 (money laundering)	B
Online Child Pornography, Child Luring, and Related Activities	18 U.S.C. § 2251 et seq. (sexual exploitation and other abuse of children) 18 U.S.C. § 2421 et seq. (transportation for illegal sexual activity)	C
Internet Sale of Prescription Drugs and Controlled Substances	15 U.S.C. § 45 et seq. (unfair or deceptive acts or practices; false advertisements) 18 U.S.C. § 545 (smuggling goods into the United States) 18 U.S.C. § 1341 et seq. (mail, wire, and bank fraud; injunctions against fraud) 21 U.S.C. § 301 et seq. (Federal Food, Drug, and Cosmetic Act) 21 U.S.C. §§ 822, 829, 841, 863, 951-971 (Drug Abuse Prevention and Control)	D
Internet Sale of Firearms	18 U.S.C. § 921 et seq. (firearms)	E
	15 U.S.C. § 3001 et seq. (Interstate Horseracing Act) 18 U.S.C. § 1084	

<p>Internet Gambling</p>	<p>(transmission of wagering information)                  18 U.S.C. §§ 1301 et seq. (lotteries)                  18 U.S.C. § 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises)                  18 U.S.C. § 1953 (interstate transportation of wagering paraphernalia)                  18 U.S.C. § 1955 (prohibition of illegal gambling businesses)                  28 U.S.C. §§ 3701-3704 (professional and amateur sports protection)</p>	<p>F</p>
<p>Internet Sale of Alcohol</p>	<p>18 U.S.C. § 1261 et seq. (liquor traffic)                  27 U.S.C. §§ 122, 204 (shipments into states for possession or sale in violation of state law)</p>	<p>G</p>
<p>Online Securities Fraud</p>	<p>15 U.S.C. § 77e, 77j, 77q, 77x, 78i, 78j, 78l, 78o, 78ff (securities fraud)</p>	<p>H</p>
<p>Software Piracy and Intellectual Property Theft</p>	<p>17 U.S.C. § 506 (criminal copyright infringement)                  17 U.S.C. § 1201 et seq. (copyright protection and management systems)                  18 U.S.C. § 545 (smuggling goods into the United States)                  18 U.S.C. §§ 1341, 1343 (frauds and swindles)                  18 U.S.C. § 1831 et seq. (protection of trade secrets)                  18 U.S.C. §§ 2318-2320 (trafficking in counterfeit labels for phonorecords, copies of computer programs or computer program documentation or packaging, and copies of motion pictures or other audio visual works)</p>	<p>I</p>

2. New Investigatory Challenges

As law enforcement agencies adapt to a more technology-based society, they need to be aware of the challenges, as well as the benefits, of online investigations. In certain circumstances, law enforcement agencies have available to them tools and capabilities created by the Internet and computers that can assist them in their fight against computer-facilitated unlawful conduct. For example, just as advances in telephone technology gave law enforcement agents the ability to determine the origin of fraudulent or threatening calls, the Internet has given law enforcement agencies the ability to find unsophisticated offenders who leave the equivalent of "fingerprints" as they commit unlawful acts. Indeed, someone who makes a threat in an Internet chat room to set off a bomb at a school and who makes little or no effort to hide his or her identity (e.g., where accurate identifying information exists for a particular "screen name") can often be traced and found with relative ease.

At the same time, law enforcement agencies must also acknowledge the growing sophistication of other computer users, who wear the equivalent of Internet gloves that may hide their fingerprints and their identity. The following is an overview of investigatory challenges – taken from actual experiences involving online investigations and discussed in greater detail in the appendices for each example of Internet-facilitated unlawful conduct – that law enforcement agencies must consider as they become more proficient with such investigations.

#### (a) *Jurisdiction*

In the physical world, one cannot visit a place without some sense of its geographic location. Whether a particular street address or an area of the world, human travel is spatially based. By contrast, because one can access a computer remotely without knowing where, in physical space, that computer is located, many people have come to think of the collection of worldwide computer linkages as "cyberspace" (a term coined by science fiction writer William Gibson). In short, cybercriminals are no longer hampered by the existence of national or international boundaries, because information and property can be easily transmitted through communications and data networks.

As a result, a criminal no longer needs to be at the actual scene of the crime (or within 1,000 miles, for that matter) to prey on his or her victims. Just as telephones were (and still are) used by traditional boiler-room operators to defraud victims from a distance, a computer server running a webpage designed to defraud senior citizens might be located in Thailand, and victims of the scam could be scattered throughout numerous different countries. A child pornographer may distribute photographs or videos via e-mail running through the communications networks of several countries before reaching the intended recipients. Likewise, evidence of a crime can be stored at a remote location, either for the purpose of concealing the crime from law enforcement and others, or simply because of the design of the network. <sup>2</sup> To be sure, the Internet increases the ability of law enforcement officials and others to detect and gather evidence from a distance. For example, a website used in a fraud scheme can be spotted from an agent's office, whereas detecting a fraudulent telemarketing or mail-fraud scheme might well require extensive field work. Long-distance detection, however, may take the investigation and prosecution of these crimes out of the exclusive purview of any single jurisdiction, thereby creating yet other challenges and obstacles to crime-solving.

For example, a cyberstalker in Brooklyn, New York may send a threatening e-mail to a person in Manhattan. If the stalker routes his communication through Argentina, France, and Norway

before reaching his victim, the New York Police Department may have to get assistance from the Office of International Affairs at the Department of Justice in Washington, D.C. which, in turn, may have to get assistance from law enforcement in (say) Buenos Aires, Paris, and Oslo just to learn that the suspect is in New York. In this example, the perpetrator needs no passport and passes through no checkpoints as he commits his crime, while law enforcement agencies are burdened with cumbersome mechanisms for international cooperation, mechanisms that often derail or slow investigations. With scores of Internet-connected countries around the world, the coordination challenges facing law enforcement are tremendous. And any delay in an investigation is critical, as a criminal's trail often ends as soon as he or she disconnects from the Internet.

This does not mean that traditional legal structures cannot be meaningfully applied to the Internet. Even though connections may be of short duration, computers are still physically located in particular places. The challenge to law enforcement is identifying that location and deciding which laws apply to what conduct. The question is how sovereign nations can meaningfully enforce national laws and procedures on a global Internet<sup>10</sup>

Inconsistent substantive criminal laws are only part of the problem, for investigative techniques are also controlled by national (or local) law. For example, law enforcement agencies must consider such issues as transborder execution of search warrants. If law enforcement agents in the United States access a computer and seize data from a computer, the fact that they have a search warrant makes that action lawful. If, with that same search warrant, they remotely access a Canadian computer (from the United States), might this constitute a criminal act under Canadian law notwithstanding the existence of the U.S. warrant? To the extent that agents know nothing more than an Internet protocol address (essentially, a series of numbers that identify a particular machine), the physical location of the computer to be searched may not be accurately known. Yet ignorance of physical location may not excuse a transborder search; consider how we would react to a foreign country's "search" of our defense-related computer systems based upon a warrant from that country's courts.

This transborder issue may raise domestic issues as well. Gambling and obscenity laws provide criminal sanctions for individuals based, in part, upon their location. One federal law prohibits transmitting information assisting in the placing of bets or wagers on sporting events or contests unless both the sender and receiver are in states or foreign countries where gambling is legal, see 18 U.S.C. §1084. Obscenity laws are also typically interpreted in light of local community standards, cf. *Miller v. California*, 413 U.S. 15 (1973). Even the search warrant provision in the federal rules requires that agents seek a warrant in the district where the property to be seized is located, see Fed. R. Crim. P. 41(a). To the extent the location of the sender, recipient, or data is unknown and perhaps unknowable, it may be difficult for law enforcement to investigate and prosecute online offenders.

#### *(b) Identification*

Another thorny issue stems from the lack of identification mechanisms on global networks, and the fact that individuals can be anonymous or take on masked identities (i.e., adopt false personas by providing inaccurate biographical information and misleading screen names). Simply stated, given the current state of technology, it can be difficult to accurately identify an individual (especially sophisticated users who take affirmative steps to hide their identity) on the Internet. As noted above, there are cases, such as the PairGain case, where law

enforcement agencies have been able to track down online criminals who leave evidence of their unlawful conduct. Over time, the ability of criminals to use technology to evade identification and the ability of law enforcement to use technology to overcome such evasion will continue to evolve. Some of the challenges of identifying perpetrators of unlawful conduct on the Internet, as well as measures taken by law enforcement and the private sector 11 to respond to such challenges, are discussed below in Part III of this report.

At the very least, there needs to be widespread and extensive training of law enforcement personnel in ways to identify those who use the Internet to commit unlawful acts. Moreover, as policymakers increasingly seek to protect certain classes of citizens, most notably minors, from unsuitable material (e.g., pornography and gambling), the potential problems of identification are evident. How can activities, such as gambling or the sale of prescription drugs or alcohol, be limited to adults when children can identify themselves as adults? Similarly, if adults can falsely identify themselves as children and lure real children into dangerous situations, how can these victims be protected?

These issues are frequently at the heart of legislative and investigative efforts. Although there have been proposals to build identification mechanisms into Internet protocols, such an approach would have to be supported by internationally-recognized, market-based, standards-making bodies whose agenda did not directly include public safety. Even if the market supported such an approach, however, such proposals are controversial, because there are strong reasons to allow anonymity in communications networks. For example, whistleblowers may wish to remain anonymous, as may a group of rape victims who wish to convene an electronic meeting to discuss their experiences without revealing their identities.

In an attempt to create a framework for evaluating identification mechanisms on the Internet, some have compared the Internet with other forms of communications, such as pay telephones and regular mail, which may offer users some degree of anonymity. Of course, the difference between these traditional means of communication and the Internet is significant, and attempting to solve Internet problems only by drawing analogies to existing technologies will often fail. The problem is that the analogies may capture some aspects of the new technology, but fail to capture others. For example, the telephone and mail systems cited above allow predominantly one-to-one communications. Although someone wishing to defame a public figure or harass others can, in theory, call thousands of people anonymously, the time and cost make this impractical. By contrast, the cost-free, simple, one-to-many nature of the Internet dramatically alters the scope and impact of communications. It is this difference which explains why children who would never spend their weekly allowance buying *The Anarchist Cookbook* at a college bookstore may download the same information from the Internet and possibly injure themselves or others testing a recipe for the making of a bomb.12 Given the complexity of this issue, balancing the need for accountability with the need for anonymity may be one of the greatest policy challenges in the years ahead.

### (c) *Evidentiary Issues*

Electronic data generated by computers and networked communications such as the Internet can be easily destroyed, deleted, or modified. Digital photographs are but one example of digital information that can be altered in ways that may be difficult to detect. As a result, law enforcement officials must be cognizant of how to gather, preserve, and authenticate electronic evidence. This will not only require substantial training of law enforcement personnel, but also sufficient experience with such evidence by investigators, prosecutors,

defense counsel, courts, and others until clear rules and standards are established. The volume of electronic evidence that requires forensic analysis is also increasing substantially. The increasing use of computers and the Internet, of course, often means that information or records of communications that were previously never retained or routinely destroyed can (in some instances) now be recovered, but such recovery may still require sophisticated computer forensics.

Thus, for the reasons noted above, law enforcement agencies face significant challenges in dealing with electronic evidence. These challenges will continue to grow, because electronic evidence can become a part of any investigation. Electronic evidence, for example, can show up as any of the following items, each presenting distinct evidentiary challenges: a drug trafficker's computerized customer records; a digital photograph of a murder scene; an encrypted e-mail containing details of a terrorist plot or fraud scheme; or a system administrator's log files of a hacker attack.

#### *(d) Infrastructure Protection*

Protecting our information infrastructure is imperative but difficult for a host of reasons: the number of different systems involved, the interdependency of these systems, the varied nature of the threats (physical and cyber, military, intelligence, criminal, natural), and the fact that many of these infrastructures are maintained primarily by the commercial sector. Addressing cyberthreats to our infrastructure is particularly difficult, because of differing views regarding our vulnerabilities; the need to balance interests relating to privacy, economic competitiveness, commercial risk, national security, and law enforcement; and the overlapping authorities within the federal government for dealing with information infrastructure issues. Although such issues are beyond the scope of this report, see National Plan for Information Systems Protection (released Jan. 7, 2000), appreciating the importance and complexity of infrastructure protection is key to understanding the needs of law enforcement in countering unlawful conduct involving the Internet (see Part III.A below).

#### *(e) Commingling*

The ability of an individual to use one computer to conduct both lawful and unlawful activities or to store both contraband and legally possessed material presents another significant issue. Such commingling defies simple solutions. The fact is, one computer can be used simultaneously as a storage device, a communications device (e.g., to send, store, or retrieve e-mail), and a publishing device. Moreover, that same computer can be used simultaneously for both lawful and unlawful ventures, and the problem becomes more complex when a single machine is shared by many users.

For example, individuals who distribute child pornography or copyrighted software using their home computers may also publish a legitimate newsletter on stamp collecting or use an e-mail service with that same computer. By seizing the computer, law enforcement agencies can stop the illegal distribution of contraband, but may, at the same time, interfere with the legitimate publication of the newsletter and the delivery of e-mail, some of which may be between users who have no connection with the illegal activity. Similarly, a doctor who is illegally prescribing drugs over the Internet may not only have on her computer evidence relating to the illegal prescriptions, but files related to her lawfully treated patients. Likewise, an attorney accused of operating an Internet sportsbook may keep in the same folder on his computer materials relating to his gambling business and documents subject to the

attorney-client privilege. Seizure of the doctor's or the lawyer's files in such circumstances could result in the seizure of legally privileged material.

### III. LAW ENFORCEMENT NEEDS AND CHALLENGES

As the examples of Internet-facilitated unlawful conduct discussed above and in the appendices illustrate, the increasing sophistication and global reach of such conduct make it all the more important to adequately equip law enforcement agencies at all levels.

The following are some of the principal issues that should be considered when evaluating how to better equip federal, state, and local law enforcement agencies to ensure the safety and security of Internet users. We urge further analysis, in consultation with state and local law enforcement, industry, and privacy and other groups, to determine the most appropriate ways to promote private sector leadership in this area and to empower law enforcement – at all levels – with the needed tools, capabilities, and legal authorities to curb unlawful conduct on the Internet while protecting privacy and supporting the growth of the electronic marketplace.

#### A. Protecting Computers and Networks

In assessing the tools, capabilities, and legal authorities needed by law enforcement to address unlawful conduct on the Internet, we must consider the larger context of how to protect the systems and networks of this Nation that make our businesses run and operate our Nation's defenses and infrastructure. As we have become more dependent on technology, our energy production and distribution channels, our transportation networks, and our telecommunication systems have become increasingly reliant on a computer-based infrastructure.

Without a protected infrastructure, there could be no conduct, lawful or unlawful, on the Internet. Electronic commerce and the marketplace cannot thrive without a strong infrastructure that the public can trust and rely upon. Consequently, proposals relating to law enforcement challenges in this area (e.g., new investigative tools, capabilities, or legal authorities) need to be assessed in light of the broader need to protect the vital infrastructure, because cyberattacks on infrastructures and other cybercrimes can lead to telecommunications breakdowns that disable electronic commerce and destroy our citizens' confidence in the Internet and computer networks.

The protection of this country's computers and networks requires everyone's cooperation. It demands a partnership among all federal agencies with responsibilities for certain special functions, such as law enforcement, intelligence, and defense.<sup>13</sup> It also requires all federal agencies to take appropriate preventive measures to protect their computer systems against attack. Most important, because the overwhelming majority of the Nation's infrastructure is in private hands, the private sector must take the steps necessary to prevent attacks against its systems.<sup>14</sup> The Partnership for Critical Infrastructure Protection, which recently held a day-long kickoff meeting, will serve as a key catalyst for this activity. In addition, we must consider the needs of state and local law enforcement, which play a critical role in fighting the cybercriminals on the street.

Meeting its responsibility to protect critical infrastructures is one of the central challenges for law enforcement as we face the 21st Century. As our reliance on the Internet, on automated systems, and on other technological advances increases with every passing month, the potential impact of attacks on critical infrastructure expands as well. Law enforcement needs to be provided the legal mechanisms and financial resources to be prepared to confront this

challenge in partnership with other federal agencies, with the private sector, and with state and local agencies. The Administration recognized this need for unprecedented cooperation between the private and public sectors in Presidential Decision Directive 63. That document provides a framework for federal agencies to cooperate with their private sector partners and for the formation of the National Infrastructure Protection Center, an interagency center for analysis, warning, and investigation of cybercrime. In addition, the Partnership for Critical Infrastructure Protection provides a cross-sectoral forum for the private sector to address a variety of infrastructure assurance issues.

## **B. Federal Tools and Capabilities**

### 1. Personnel, Equipment, and Training

In 1986, an astronomer-turned-systems-manager at the University of California at Berkeley found a 75-cent accounting error in a computer's billing program, which led to the discovery that an unauthorized user had penetrated Berkeley's computer system. When the astronomer, Clifford Stoll, began to investigate further, he discovered that a hacker identified as "Hunter" was using Berkeley's computer system as a conduit to break into U.S. government systems and steal sensitive military information. The hacker's objective seemed to be to attain U.S. anti-ballistic missile technology.

As he began to pursue the hacker, Stoll encountered serious problems. To begin with, Stoll was unable to find computer-literate law enforcement personnel with an appreciation of the technical nature of the criminal activity. Local and federal agencies that Stoll contacted, including the FBI and CIA, initially expressed little interest in pursuing what at first looked like a computer prank. (Moreover, until government investigators learned of the potential threat to national security, they had no interest in pursuing a case which appeared to have damages valued at less than one dollar.) Because Hunter's trail vanished each time he ended a communication, he could only be traced when he was online. But because it was often after business hours (and, indeed, sometimes in the middle of the night) when Hunter attacked, there were few (if any) law enforcement personnel available during those sessions. The call was eventually traced to Germany, but adding an international element to the case now meant that it was usually after business hours in at least one time zone where the communication was passing through. Stoll cleverly resorted to generating phony official-looking data to keep the hacker interested and online long enough for the trace to be completed. Eventually, the source of the attacks was identified as a German hacker, and he was successfully prosecuted there.<sup>15</sup>

Ironically, one reason this investigation was successful is that Stoll did not rely solely on law enforcement, but instead was able to work directly with telephone company personnel, who in turn worked with other telecommunications providers. His investigation brought to light a number of interdependent personnel and resource requirements that, unless fulfilled, will impede the success of law enforcement in this area. Despite significant progress since the time of this example, it remains a useful illustration of some of the fundamental issues that continue to need further attention at the domestic and international level to eliminate weak links in the chain of an investigation.

#### *(a) Experts Dedicated to High-tech Crime*

The complex technical and legal issues raised by computer-related crime require that each jurisdiction have individuals who are dedicated to high-tech crime and who have a firm

understanding of computers and telecommunications. The complexity of these technologies, and their constant and rapid change, mean that investigating and prosecuting offices must designate investigators and prosecutors to work these cases on a full-time basis, immersing themselves in computer-related investigations and prosecutions. Many agencies, including the Departments of Justice, Treasury, and others, have already dedicated available resources to do so. The Federal Trade Commission ("FTC") adopted this approach when it formed an Internet Rapid Response Team and successfully halted several online fraud schemes in a matter of weeks. Some federal agency inspectors general have also established computer crime divisions, complete with forensics laboratories and technical experts, and many have information technology audit and inspection capabilities to assist their agencies in identifying vulnerabilities, best practices, and other critical infrastructure issues.

But more of such expertise and the resources to support the increasing cyber-workload are needed. Indeed, each state attorney general's office, each U.S. Attorney's office, each federal law enforcement squad, and each country's equivalent to the U.S. Department of Justice should have a dedicated high-tech crime unit that knows how to respond to a fast-breaking investigation and that knows who else to contact in the chain of a communication and how to reach those individuals. These experts will also be needed to support other law enforcement authorities faced with high-tech issues, such as when a computer is used to facilitate an otherwise traditional crime.

The Department of Justice has designated a prosecutor in each U.S. Attorney's Office to serve as a computer and telecommunications coordinator for that district, and the FBI has established the National Infrastructure Protection Center and the National Infrastructure Protection and Computer Intrusion program. Staffing levels for these programs are below the level needed to effectively address the concerns raised in this report. Given the magnitude of the challenges, the continually changing technology, and the complexity of these investigations, these are necessarily resource-intensive programs.

*(b) Experts Available on a 24-Hour Basis*

A unique feature of high-tech and computer-related crime is that it often requires immediate action to locate and identify criminals. The trail of a criminal may be impossible to trace once a communication link is terminated, because the carrier may not keep (or is not required by law to keep) records concerning each individual communication. This lack of information is due, in part, to the fact that there often is no longer a revenue-related reason for recording transmission information (i.e., connection times or source and destination) for individual connections. For example, many businesses no longer bill their customers by individual telephone call or Internet connection but, instead, by bulk billing (e.g., a single rate for one month of usage). When a carrier does not collect traffic data, a suspect's trail may evaporate as soon as the communication terminates.

Therefore, investigators and prosecutors with expertise in this field must be available 24 hours a day so that appropriate steps can be taken in a fast-breaking high-tech case. For example, the National Infrastructure Protection Center operates a 24-hour/7-day-a-week command post for around-the-clock coverage of computer intrusion matters. And, Attorney General Reno recently challenged the National Association of Attorneys General to work with the Department of Justice and other appropriate organizations (among other things) to create a 24/7 network of computer crime enforcement personnel in every state.<sup>16</sup>

### *(c) Regular and Frequent Training*

Because of the speed at which communications technologies and computers evolve, and because criminal methods in these areas generally change more rapidly than those in more traditional areas of crime, experts must receive regular and frequent training in the investigation and prosecution of high-tech cases. Programs such as those offered by the FBI at its Quantico facility and elsewhere and under the National Cybercrime Training Partnership provide such training to federal, state, and local law enforcement personnel, but more is needed. Government computer professionals, such as systems operators and administrators, also need regular and frequent training, because they are often the first to detect unlawful conduct that targets federal computer systems.

In addition to domestic training, countries should participate in coordinated training with other countries, so transnational cases can be pursued quickly and seamlessly. By way of example, in the U.S., high-tech prosecutors at the federal level attend a 1-week training course every year, with training provided by both government and private sector personnel. Likewise, in 1998, the G-8 countries held an international high-tech training conference for its countries' law enforcement personnel.

### *(d) Up-to-date Equipment*

In the past, a police officer would be given a gun, a flashlight, and a notepad when he or she was hired. Twenty years later, the three items would be returned to the police department when the officer retired, and the only intervening equipment expenses would have had to do with replacement bullets, batteries, and note paper. Today, keeping pace with computer criminals means that law enforcement experts in this field must be properly equipped with the latest hardware and software. Providing proper equipment, however, can be one of the more difficult challenges, because the cost of purchasing and upgrading sophisticated equipment and software places considerable burdens on the budget process.

Ultimately, personnel, training, and equipment needs require the direct involvement of senior officials, such as the Attorney General and FBI Director, because of the budget-request and budget-allocation processes that are involved with such expenditures. Moreover, in many jurisdictions, senior policymakers may not be as familiar with new computer and telecommunications technologies and with threats posed by cybercriminals. If senior government officials in those jurisdictions are unfamiliar with the technologies at issue or the new threats and challenges they pose, they may be hesitant to support law enforcement by seeking appropriate legislative and budgetary changes. The need for adequate personnel, resources, and training is thus a critical issue in this increasingly important area of law enforcement.

## Encryption and the Challenge of Unlawful Conduct on the Internet

The practice of encryption, sometimes called cryptography, is the use of mathematical or other methods to hide the content of messages or files. Encryption often uses a secret key — a word, phrase, or other information that is not easily guessed — to ensure that only those who know the key can read the content of the file or message. Cryptography has been studied and practiced by governments and militaries for centuries, but only in the last decade have individuals begun to encrypt large amounts of data using computers. Today, encryption can be used to secure both communications over networks and stored data on computers.

Encryption now presents and will continue to present a challenge to law enforcement confronting Internet-related crime. Robust encryption products make it difficult or impossible for law enforcement to collect usable evidence using traditional methods, such as court-authorized wiretaps and search warrants. Moreover, as encryption tools are increasingly built into retail software and hardware products, the use of encryption will require little skill or effort for users to implement. As a result, lawbreakers can communicate and store information relating to crimes with little fear that police can discover and use that information. Increasing limitations on law enforcement's ability to detect, investigate, and prove certain types of crime may place the public safety at a correspondingly increased risk.

By the same token, encryption has many positive aspects which assist in protecting users of the Internet from crime. Companies use encryption to enhance protection of their proprietary data, so that even if their networks are penetrated by a hacker, the information stored on the network will be meaningless to the intruder. Similarly, individuals and merchants use cryptography to help protect sensitive personal data (such as credit card numbers) from being revealed to outsiders during transactions over a network. Finally, in coming years, individuals will use products and services based upon cryptography to ensure that the person or organization with whom they are communicating is authentic, thus reducing fraud and identity theft.

The immediate challenge for law enforcement is finding ways to promote the many positive aspects of encryption while maintaining the current ability to prevent and prosecute crime. To do this, federal, state, and local law enforcement agencies will have to enhance their understanding of encryption tools and develop techniques for obtaining evidence despite their use by criminals. By working with industry, privacy groups, and others, we will continue to look for solutions that harmonize society's interests in protecting privacy and protection from crime.

## 2. Locating and Identifying Cybercriminals

When a hacker disrupts air traffic control at a local airport, when a cyberstalker sends a threatening e-mail to a public school or a local church, or when credit card numbers are stolen from a company engaged in e-commerce, investigators must locate the source of the communication. To accomplish this, they must trace the "electronic trail" leading from the victim back to the perpetrator. But the realities for law enforcement engaged in such a pursuit are very different from those of just a few years ago. Consequently, society faces significant challenges in the coming years as online criminals become more sophisticated and as technology may make anonymity more easily available. The following are some of the challenges facing both industry and law enforcement.

*Divested and Diverse Environment.* In today's communications environment, where telecommunication services are no longer provided by a monopoly carrier, a single end-to-end transmission is often carried by more than one carrier. As a result, the communications of a hacker or other criminal may pass through as many as a dozen (or more) different types of

carriers, each with different technologies (e.g., local telephone companies, long-distance carriers, Internet service providers ("ISPs"), and wireless and satellite networks). The communication may also pass through carriers in a number of different countries, each in different time zones and subject to different legal systems. Indeed, each of these complications may exist within a single transmission. This phenomenon makes it more difficult (and sometimes impossible) to track criminals who are technologically savvy enough to hide their location and identity.

*Wireless and Satellite Communications.* Cellular and satellite-based telephone networks allow users to roam almost anywhere in the world using the same telephone. Although the social and commercial benefits of such networks are obvious, these networks can also provide a valuable communication tool for criminal use. Although sophisticated technology may allow law enforcement, under certain circumstances, to identify the general geographic region from which a wireless call is originating or terminating, the use of such technology raises profound and difficult issues at the intersection of privacy and law enforcement policies. Moreover, even identifying the owner of a particular mobile phone can be difficult, because mobile phones can be altered to transmit false identifying information. As the costs of mobile phones and mobile telephony service drop, we can expect to see the marketing of more "disposable phones," which will further complicate the ability of law enforcement agencies to gather evidence linking a perpetrator to the communication.

Satellite telephony presents additional issues. Current satellite-based networks transmit communications from users through one or more satellites and to earth-based gateways where the communications are routed using land-line systems. Providers of satellite-based telephony services typically do not need to build a gateway in each country to which service is to be provided. Indeed, it may be the case that one or two gateways can service an entire continent. The government's ability to protect the public's safety and privacy can be threatened in instances where a gateway servicing U.S. customers is located outside the U.S. In such cases, the content of the communications, as well as identifying information about the callers themselves, will be subject to the relevant laws (if any) of the host country and may not be protected in the same manner that the information is protected in the United States. More importantly to law enforcement, the location of a gateway in another country makes it difficult for law enforcement to meet its obligation to protect against criminal activities. In addition, law enforcement may have to rely on the willingness and technical and legal ability of the country in which the gateway is located to trace telephone calls, obtain information regarding suspected criminals in the United States, and provide that information to U.S. law enforcement agencies.

Recognizing the benefits and challenges created by advances in global telephony, the federal government has been working with telecommunications companies and foreign law enforcement agencies to ensure that the public interest is served in a global telephony environment. The government is also addressing global telecommunications issues in various international fora to ensure that the U.S. retains its ability to protect the U.S. public's privacy and safety.

*Real-time Tracing.* Tracing a communication from victim back to attacker may be possible only when the attacker actually is online. Sophisticated criminals can alter data concerning the source and destination of their communications, or they may use the Internet account of another. In addition, transmission information may not be retained or recorded by communications providers or may not be captured at all or held for only a short period of

time. Even if it is generated and retained, it might be deleted by a skilled intruder to hide his identity.

Consequently, when law enforcement officials have information that a crime is being committed online, they often must attempt to trace a communication as it occurs. To do so, a law enforcement agency must know which computer crime expert to call in which jurisdiction, be able to contact the relevant individuals at various ISPs and carriers, and secure appropriate legal orders in each jurisdiction where a relevant carrier or ISP is located. (Notably, many ISPs already coordinate and cooperate with law enforcement agencies in this respect, and industry groups are developing "best practices" to encourage others to do the same.) Critical personnel must also be available when network-facilitated crimes occur after business hours. When these crimes occur across borders, real-time investigations must be able to proceed on an international scale.

*Technical Infrastructure and Data Retention.* If the communications network and the computers and software that run it have not been designed and configured to generate and preserve critical traffic data, information relating to the source and destination of a cyber-attack will likely not exist. Consider, for example, the use by many ISPs of modem banks to provide Internet access to incoming callers. An ISP may have 2 million customers, but maintain only 100,000 phone lines, based on an expectation that no more than 100,000 customers will ever dial in at any given time. The ISP may give only one access number to its customers and dynamically assign each incoming call to the next available line. Without a revenue-related reason for knowing the specific line used for each connection, the ISP's network may not be designed to generate the data necessary to link a customer with a specific incoming line. This, in turn, may make it impossible to trace the origin of the telephone call into the ISP's network. Such a network design can make it difficult to obtain traffic data critical to an investigation.

Even if a particular piece of the technical infrastructure is capable of generating and preserving needed data, such data are not useful if carriers do not collect and retain such records.<sup>17</sup> Issues concerning whether, to what extent, and for how long critical data are retained are decided both by national laws (or the lack thereof) and by industry practices, which generally reflect market preferences and other revenue-related needs.<sup>18</sup> In examining data retention practices and laws, careful consideration must be given to privacy concerns, market realities, and public safety needs.

U.S. law enforcement may be significantly affected by the 1995 and 1997 directives of the European Union ("EU") concerning the processing of personal data, including the deletion of traffic data. EU Member States are in the process of developing implementing legislation.<sup>19</sup> As the directives are implemented into national legislation throughout the EU, it is vital that public safety be considered, along with the privacy and market force elements.

*Anonymity.* Anonymous e-mail accounts, which are e-mail accounts where subscriber information is not requested or verified, <sup>20</sup> are the proverbial double-edged sword. Such anonymous accounts can protect privacy, but they add new complexities to identifying online lawbreakers, such as individuals who send child pornography, death threats, computer viruses, or copyright-protected works by e-mail.

Similarly, "anonymous re-mailer" services, which are e-mail services that strip the source address information from e-mail messages before passing them along to their intended

recipients, raise difficult privacy and law enforcement policy issues. On the one hand, anonymous re-mailer services provide privacy and encourage freedom of expression. For example, in early 1999, these services allowed ethnic Albanians to provide first-hand accounts of Serbian atrocities in Kosovo without the fear of retribution. On the other hand, such services can plainly frustrate legitimate law enforcement efforts. Indeed, as early as 1996, one such service expressly touted itself as "a way to thwart attempts by intelligence agencies to trace illegal traffic . . . . It holds all incoming messages until five minutes after the hour, then re-mails them in random order. The messages are sent through five to twenty other re-mailers, with a stop in at least one of the several countries noted for lax law enforcement." 21

To be sure, individuals can generally engage in many "real world" activities relatively anonymously, such as making small cash payments and attending public events. But they cannot remain anonymous in other contexts, such as opening a bank account or registering a car. Indeed, many financial institutions have substantial customer identification requirements. As discussed in Part II.B above, Internet-based activities should be treated consistently with physical world activities and in a technology-neutral way to further important societal goals (such as the deterrence and punishment of those who commit money laundering). National policies concerning anonymity and accountability on the Internet thus need to be developed in a way that takes account of privacy, authentication, and public safety concerns.

### 3. Collecting Evidence

When computers are used to store information, law enforcement agents generally can, upon securing a warrant, search the computer in the same way that they would a briefcase or file cabinet. The difference, of course, is that a computer can store a tremendous amount of information, including evidence that might not be known to the computer's owner. 22 This feature of computer information can, of course, be both a benefit to and a challenge for law enforcement. It can benefit law enforcement by providing information (sometimes in a readily searchable way) that might not have existed in the non-computer world. But it can obviously present law enforcement challenges by highlighting the need for training and expertise (and time) for the information to be recovered. For example, one computer with 3 gigabytes of memory can contain the equivalent of one million pages of information. "Keyword" searches can miss relevant information, and the difficulty of the search and recovery of information may depend on how familiar the forensic expert is with the particular hardware and software configuration of the computer at issue. Moreover, if information on the computer is encrypted, it may be completely inaccessible to law enforcement and contribute little to solving the crime at issue (see box on encryption).

### C. State and Local Tools and Capabilities

State and local law enforcement agencies play a significant role in addressing unlawful conduct on the Internet. These agencies have been crucial in combating online child pornography, prescription drug sales, gambling, and fraud. Consequently, any initiatives by the federal government to address unlawful conduct on the Internet must account for the important role state and local governments play in online investigations and prosecutions and should address the following three areas of fundamental concern to these state and local law enforcement authorities: (1)jurisdiction; (2)cooperation and coordination; and (3)resources.

The following is a brief discussion of the jurisdictional, cooperation and coordination, and

resources issues facing state and local governments. Because the Executive Order that prompted this report focuses on federal law enforcement issues, we recommend that a more detailed analysis of state and local law enforcement issues be undertaken as a next step.

### 1. Jurisdiction

In responding to the challenge of law enforcement on the Internet, one of the problems that state and local governments face is that, although the crimes and schemes on the Internet may victimize local populations, the medium over which these crimes are committed permits a defendant to be located anywhere in the world. The traditional investigative tools available to the state – interviews, physical or electronic surveillance, and service of subpoenas for the production of documents or for testimony – are not necessarily adequate to compel information from a wrongdoer who is located out of state.

For example, if a fraud scheme is committed against Ohio residents by an operator of a website located in Florida, and the Ohio prosecutors issue a subpoena for records from the company in Florida, there is currently no formal procedural mechanism for the service and enforcement of that subpoena. Although the Ohio prosecutors may informally succeed in obtaining assistance from the Florida authorities, this is a matter of professional courtesy rather than legal process. There is no guarantee that the subpoena will be served, or, if served, enforced. Running into such a roadblock could well mean the end of the Ohio investigation. In the absence of any ability to investigate the case themselves, it remains possible for the Ohio prosecutors simply to refer the case to their Florida counterparts by reporting their complaints about the cybercriminal in Florida, but if the crime involves no Florida victims or is otherwise outside its jurisdiction, there is no guarantee that the case will be investigated by anyone.

This example illustrates the kinds of jurisdictional hurdles that are becoming increasingly common for state and local law enforcement authorities pursuing crime over the Internet. Another difficulty in this area arises from the disparate approaches taken by state courts to whether a state can exert long-arm jurisdiction over an Internet site accessible in that state. The lack of uniformity may make it more difficult for investigators in some jurisdictions to conduct meaningful investigations of Internet conduct. And, the enforcement of state electronic surveillance orders can also be a challenge. The Internet and modern satellite communications have made it more necessary for state wiretap orders to be served on and enforced against an out-of-state service provider. Unfortunately, no legal mechanism exists that would allow this. For example, drug traffickers operating entirely in New York, but using satellite telephones with signals that are received at a ground station outside of New York, potentially are completely immune from a New York wiretap order if the out-of-state ground station refuses to comply with a New York court's wiretap order.

### 2. Interstate and Federal-State Cooperation

Because the gathering of information in other jurisdictions and internationally will be crucial to investigating and prosecuting cybercrimes, all levels of government will need to develop concrete and reliable mechanisms for cooperating with each other. The very nature of the Internet – its potential for anonymity and its vast scope – may cause one law enforcement agency to investigate, inadvertently, the activities of another agency that is conducting an undercover operation. Likewise, the law enforcement agency of one state may require the assistance of another for capturing and extraditing a criminal to its state for prosecution. In

other words, crimes that were once planned and executed in a single jurisdiction are now planned in one jurisdiction and executed in another, with victims throughout the United States and the world.

The effective coordination and cooperation between various branches of the law enforcement community is crucial to any effort to combat unlawful conduct on the Internet. One area that may deserve further review concerns the extent to which federal, state, and local authorities can share and gather information about pending cases, potential targets, investigative procedures and tactics, and contact personnel. Such coordination is necessary for federal, state, and local law enforcement agencies to avoid duplicating and possibly undermining investigations.

In January 2000, Attorney General Reno challenged the National Association of Attorneys General and other state and local law enforcement groups to make it a priority to respond to these significant needs. Among other things, she specifically urged the groups to:

- Create a 24-hour cybercrime point of contact network, where each participating federal, state, and local law enforcement agency would provide a designated contact who is available 24 hours per day, 7 days per week to assist with cybercrime issues. This contact could be available via a pager system or coordinated through a centralized "command center."
- Create an online clearinghouse for sharing information to avoid duplication of effort and multiple investigations of the same unlawful conduct. Existing mechanisms, such as XSP, LEO, or Consumer Sentinel, may either serve this function or serve as building blocks for such a service.
- Develop conferences for all state and local Internet investigators and prosecutors, yearly or bi-annually, at which recent developments are discussed, case progress shared, and networks reinforced that will facilitate state, federal, and local cooperation.
- Develop additional policies and mechanisms to enhance cooperative interstate investigative and prosecutorial capacities and encourage coordination among their constituents.

### 3. Resources

Although state and local law enforcement organizations are responsible for investigating and prosecuting most forms of unlawful conduct involving the use of the Internet, they have limited resources with which to pay the substantial costs of developing the technical, investigative, and prosecutorial expertise and acquiring the new and often expensive technology necessary to address these crimes. Personnel, equipment, and training must be funded not only once but on a recurring basis. In addition, the structure of state and local law enforcement agencies is different from state to state and even county to county within a state. Resources must not be so restricted as to prohibit a state or local government from tailoring programs and initiatives within their current structures.

Federal funding can be useful in supplementing state and local spending on the necessary personnel, training, and equipment to properly investigate and prosecute high technology

crime cases. To the extent that federal funds are expended on enhancing federal law enforcement's forensic capabilities, these projects should be structured in a way that allows state and local law enforcement to use these forensic resources. Regional computer forensic laboratories, such as the new laboratory in San Diego, have been successful and may be a model for other such facilities. 23

#### **D. Legal Authorities: Gaps in Domestic Laws**

Law enforcement agencies need strong laws to protect society against unlawful activity. This is as true in the online world as it is in the offline world. As discussed above in Part II and detailed in the appendices to this report, existing federal law is generally adequate to cover unlawful conduct involving the use of the Internet.

Strong substantive laws, however, that apply to the use of the Internet to commit traditional offenses such as fraud, child pornography, gambling, and the illegal sale of intellectual property are necessary but not sufficient to ensure a safe and secure online environment. To achieve that goal, law enforcement, in cooperation with the private sector, must also be able to gather evidence, investigate, and prosecute these cases. Unfortunately, in some areas, the legal authorities and tools needed to do this have lagged behind technological and social changes. This section examines several laws related to the investigation and prosecution of high-tech offenses that have not kept pace with technological changes. Although we do not offer specific solutions in this report, we are committed to working with interested parties to devise appropriate solutions.

##### 1. Pen Register and Trap and Trace Statute

Pen registers (devices that record the numbers dialed on a telephone line) and trap and trace devices (devices that capture incoming electronic impulses that identify the originating number) are important tools in the investigation of unlawful conduct on the Internet. Unfortunately, the statute that governs such devices, 18 U.S.C. §§ 3121-3127, is not technology-neutral and has become outdated.

As an initial matter, advances in telecommunications technology have made the language of the statute obsolete. The statute, for example, refers to a "device" that is "attached" to a telephone "line," *id.* § 3127(3). Telephone companies, however, no longer accomplish these functions using physical hardware attached to actual telephone lines. Moreover, the statute focuses specifically on telephone "numbers," *id.*, a concept made out-of-date by the need to trace communications over the Internet that may use other means to identify users' accounts.

Moreover, the deregulation of the telecommunications industry has created unprecedented hurdles in tracing long-distance telephone calls. Many different companies, located in a variety of judicial districts, may handle a single call. Under the existing statute, however, a court can only order communications carriers within its district to provide tracing information to law enforcement. As a result, investigators have to apply for several, sometimes many, court orders to trace a single communication, causing needless waste of time and resources and hampering important investigations.

##### 2. Computer Fraud and Abuse Act

Originally passed in 1984, and amended in 1986, 1994, and 1996, the Computer Fraud and

Abuse Act, 18 U.S.C. § 1030, protects a broad range of computers that facilitate interstate and international commerce and communications. For example, section 1030(a)(2) makes it a crime to access a computer without or in excess of authority and obtain (1) financial information from a financial institution or credit reporting company; (2) any information in the possession of the government; or (3) any private information where the defendant's conduct involves interstate or foreign commerce. Section 1030(a)(5) makes it a crime for anyone to knowingly cause the transmission of a computer program, information, code, or command, that results in unauthorized damage to a protected computer. (A "protected computer" is one used exclusively or partly by the United States or a financial institution in which the defendant's conduct affects the government's or financial institution's operation of the computer; or any computer that is used in interstate or foreign commerce or communications, see 18 U.S.C. § 1030(e)(2).) 24

Despite its broad reach and relatively recent amendment, the statute nevertheless contains several flaws that could hinder law enforcement's ability to respond effectively to unlawful conduct on the Internet. For example, given the increasing interdependency and availability of global computer networks, it is increasingly likely that computer system intruders within the United States may begin to concentrate their unlawful activity on systems located entirely outside the United States. Alternatively, individuals in foreign countries may route communications through systems located within the United States, even as they hack from one foreign country to another. In such cases, they may hope that the lack of any U.S. victim would either prevent or discourage U.S. law enforcement agencies from assisting in any foreign investigation or prosecution. It is unclear whether section 1030, in its existing form, protects against such situations, which may affect the United States even though the perpetrator and the victim are located elsewhere.

The Department of Justice has encountered several instances where intruders have attempted to damage critical systems used in furtherance of the administration of justice, national defense, or national security, as well as systems (whether publicly or privately owned) that are used in the provision of "critical infrastructure" services such as telecommunications, transportation, or various financial services, but where proof of damage in excess of \$5,000, as required by section 1030(a)(5), has not been readily available. Although such activities may pose extreme risks to our infrastructure, section 1030(a)(5) currently does not allow law enforcement to proceed without evidence of over \$5,000 in damages.

Another problem is that prosecutions under section 1030(a)(5) carry a mandatory minimum sentence of at least six months. In some instances, prosecutors have exercised their discretion and elected not to charge some defendants whose actions otherwise would qualify them for prosecution under that section, knowing that the result would be mandatory imprisonment. It may be useful to examine whether requiring imprisonment for six months should be applied in more limited circumstances than allowed under existing law, or whether other punishments, such as reduced penalties and forfeiture of any instrumentalities or proceeds of the violation, might provide adequate punishment and deterrence.

### 3. Privacy Protection Act

The Privacy Protection Act of 1980 ("PPA"), 42 U.S.C. §2000aa, et seq., makes it unlawful for local, state, or federal law enforcement authorities to "search for or seize any work product materials" or any "documentary materials . . . possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of

public communication," 42 U.S.C. § 2000aa(a), (b) (emphasis added). The statute defines "work product materials" as materials prepared or possessed in anticipation of communicating such materials to the public, except if the materials constitute contraband or the fruits or instrumentalities of crime. *Id.* § 2000aa-7(b). "Documentary materials," on the other hand, consist of materials upon which information is recorded, once again with the exception of contraband and the fruits or instrumentalities of crime. *Id.* § 2000aa-7(a).

In enacting the PPA, Congress restricted searches for evidence of crime held by innocent third-parties who were engaged in First Amendment-protected activities. The PPA thus protects the confidentiality of non-evidentiary files held by this special group of innocent third-parties – such as drafts of articles not yet published and the research and other supporting information (e.g., notes and interviews) that are never intended to be published. To preserve the confidentiality of these designated materials, the PPA instructs investigators not to search for the evidence at all, but to compel the innocent third-parties to find and produce it themselves. Thus, subject to certain exceptions, the PPA generally limits searches for work-product and documentary materials held by third-parties who plan to use them to communicate to the public.

New issues arise with the PPA due to the exponential growth in computer use over the last decade. With the advent of the Internet and widespread computer use, almost any computer can be used to "publish" material. As a result, the PPA may now apply to almost any search of any computer. Because computers now commonly contain enormous data storage devices, wrongdoers can use them to store material for publication – material that the PPA protects – while simultaneously storing (in a commingled fashion) child pornography, stolen classified documents, or other contraband or evidence of crime.

#### 4. Electronic Communications Privacy Act

In 1986, Congress enacted the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 et seq., in an effort to revise and expand the scope of the 1968 wiretap act. The statute attempted to strike a workable balance among the competing interests addressed in the statute at the time: the privacy interests of telecommunications users, the business interests of service providers, and the legitimate needs of government investigators.

Two factors have raised concerns about ECPA: (1) the statute treats wire and electronic communications inconsistently; and (2) use of the Internet has grown dramatically, and voice and non-voice data have converged. First, although ECPA attempted to create a technology-neutral framework for regulating the disclosure of electronic communications and records, it was only partially successful. For example, the 1986 legislation distinguished broadly between "wire communications" (such as voice telephone calls) and "electronic communications," which it accorded lesser protections. This inconsistency create practical problems in today's converged network environment where voice and non-voice data may be intertwined in a single data stream.

These inconsistencies take on additional significance with the now widespread use of computers and the Internet, because the proportion of criminal activity occurring online, or using telecommunications technologies, has increased over time. E-mail, voice mail, user access logs, and remotely stored files play an important, and in many cases, critical role in investigating and prosecuting crimes ranging from large-scale consumer fraud to extortion and murder.

These developments suggest that ECPA be carefully evaluated to ensure that it (1) takes into account new communications technologies in its treatment of wire and electronic communications; (2) has appropriate penalties for a variety of criminal invasions of communications privacy; (3) resolves deficiencies in the rules for government access to customer records, especially with respect to access by civil and regulatory agencies; and (4) cures omissions and inconsistencies within the statutory framework.

#### 5. Telephone Harassment

The Internet and the widespread use of computers have created a host of new tools for communication. Existing statutes provide criminal penalties for persons who use telephones to harass or abuse others. For example, one provision of 47 U.S.C. § 223 makes it a federal crime, punishable by up to two years in prison, to use a telephone or telecommunications device to annoy, abuse, harass, or threaten any person at the called number. The statutory prohibition applies only if the perpetrator does not reveal his or her name. See 47 U.S.C. § 223(a)(1)(C).

The new means of communication by computer, however, have given computer users a new method of inflicting such abuse not covered by the existing laws. A malicious computer user, for example, can post an electronic message in which he pretends to be the person that he intends to harass (see cyberstalking box in Part II.A above). In this fraudulent message (that may reach thousands of people), he can state, for example, that he (posing as the victim) likes to participate in some particular sexual act and then invite anyone who reads the message to call the victim's home telephone number. Yet this form of harassment evades the prohibitions of 47 U.S.C. § 223, which applies only to direct communications between the perpetrator and the victim.

#### 6. Cable Communications Policy Act

The Cable Communications Policy Act of 1984, which regulates various aspects of the cable television industry, includes provisions that protect the privacy of individual cable subscribers' records. See 47 U.S.C. § 551(e), (h). Such records should indeed remain private under most circumstances. The statute, however, did not take into account the changes in technology that have occurred over the last 15 years. Cable television companies now often provide Internet access and telephone service in addition to television programming. Some cable companies have interpreted the statute as overriding their obligations to disclose certain records pursuant to other statutes, such as the Electronic Communications Privacy Act, 18 U.S.C. § 2701, and the trap and trace statute, 18 U.S.C. § 3121. This interpretation – which courts have not accepted – would create greater protections for subscribers who receive Internet service from cable companies than for those who access the Internet by other methods.

Such an interpretation is inconsistent with the technology-neutrality principle discussed in section II.B above. Moreover, some cable companies that provide Internet service have relied on the Act to refuse to disclose subscriber information pursuant to state grand jury subpoenas, even though these records would otherwise be available through legal process under existing law. As more and more Internet users shift to high-speed cable access from traditional analog telephone equipment, it will be important to ensure that privacy standards are harmonized for all Internet users.

\* \* \*

These examples are only some of the areas in which the law has not kept up with new technology. Specific legislative proposals to update these laws are beyond the scope of this report. The gaps illuminate, however, the investigatory challenges posed by the use of the Internet for unlawful conduct, and they deserve prompt legislative consideration and attention.

## **E. Challenges for International Cooperation**

### **1. Substantive International Criminal Law**

When one country's laws criminalize high-tech and computer-related crime and another country's laws do not, cooperation to solve a crime, as well as the possibility of extraditing the criminal to stand trial, may not be possible. Inadequate regimes for international legal assistance and extradition can therefore, in effect, shield criminals from law enforcement: criminals can go unpunished in one country, while they thwart the efforts of other countries to protect their citizens.

International legal assistance can be requested and provided through several means. The United States is party to over 20 bilateral mutual legal assistance treaties ("MLATs"). Where there is no MLAT in force, international legal assistance is governed by domestic mutual legal assistance laws and practices, which include the letters rogatory process. (A letter rogatory is a letter request for assistance from one country's judicial authority – e.g., a U.S. District Court – to that of another country. See, e.g., 28 U.S.C. § 1782.) MLATs and domestic laws vary with regard to the requirements relating to a request for assistance. To issue subpoenas, interview witnesses, or produce documents, some MLATs and some laws permit assistance as long as the conduct under investigation is a crime in the requesting state, even where it is not also a crime in the requested state.

In the more sensitive area of searches and seizures, however, dual criminality (i.e., that the conduct under investigation is a crime in both the requesting and requested countries and is punishable by at least one year in prison) is often required (e.g., U.S./Netherlands MLAT). In other circumstances, a country can refuse a request if the request "relates to conduct in respect of which powers of search and seizure would not be exercisable in the territory of the Requested Party in similar circumstances" (e.g., U.S./U.K. MLAT). Finally, some MLATs and domestic laws permit assistance only if dual criminality exists and if the offense is extraditable (e.g., mutual assistance laws of Germany). With regard to extradition, the United States has entered into bilateral treaties with over 100 countries. These treaties are either "list treaties," containing a list of offenses for which extradition is available, or they require dual criminality and that the offense be punishable by a specified minimum period. Therefore, if one country does not criminalize computer misuse (or provide for sufficient punishment), extradition may be prohibited.

The issue of dual criminality is not an academic or theoretical matter. In 1992, for example, hackers from Switzerland attacked the San Diego Supercomputer Center. The U.S. sought help from the Swiss, but the investigation was stymied due to lack of dual criminality (i.e., the two nations did not have similar laws banning the conduct), which in turn impeded official cooperation. Before long, the hacking stopped, the trail went cold, and the case had to be closed.

The solution to the problems stemming from inadequate laws is simple to state, but not as

easy to implement: countries need to reach a consensus as to which computer and technology-related activities should be criminalized, and then commit to taking appropriate domestic actions. Unfortunately, a true international "consensus" concerning the activities that universally should be criminalized is likely to take time to develop. Even after a consensus is reached, individual countries that lack appropriate legislation will each have to pass new laws, an often time-consuming and iterative process.

## 2. Multilateral Efforts

Although bilateral cooperation is important in pursuing investigations concerning unlawful conduct involving the use of the Internet, multilateral efforts are a more effective way to develop international policy and cooperation in this area. The reason for this stems from the nature of the Internet itself. Because Internet access is available in over 200 countries, and because criminals can route their communications through any of these countries, law enforcement challenges must be addressed on as broad a basis as possible, because law enforcement assistance may be required from any Internet-connected country. That is, even if two countries were able to resolve all the high-tech crime issues they faced, they would still (presumably) only be able to solve those crimes that involved their two countries. Multilateral fora allow many countries to seek solutions that will be compatible to the greatest extent with each country's domestic laws.

Several multilateral groups currently are addressing high-tech and computer-related crime. Of these groups, the Council of Europe ("COE"), and the Group of Eight ("G-8") countries are the most active. To begin to address the need to harmonize countries' computer crime laws, the COE is drafting a Cybercrime Convention, which will define cybercrime offenses and address such topics as jurisdiction, international cooperation, and search and seizure. The Convention may be completed as soon as December 2000. After approval by a high-level committee, the Convention will be open for signature by COE members and non-member states which participated in the drafting. The G-8 Subgroup on High-tech Crime has been focusing on ways to enhance the abilities of law enforcement agencies to investigate and to prosecute computer- and Internet-facilitated crimes, such as establishing a global network of high-tech crime experts and developing capabilities to locate and identify those who use the Internet to commit crimes. In May 1998, President Clinton and his G-8 counterparts adopted a set of principles and an action plan, developed by the Subgroup, for fighting computer crime. The COE and G-8 efforts, as well as other international efforts, are described in more detail in Appendix J to this report.

## 3. Continuing Need for International Cooperation

As these multilateral efforts progress and as more formal mechanisms for cooperation are developed, law enforcement agencies in the U.S. and other countries are cooperating informally and have undertaken joint initiatives to achieve their goals. For example, the Customs Service has been involved in joint cyber-investigations with the German Federal police. These joint investigations have resulted in 24 referrals from Customs' Cybersmuggling Center to field offices during the last three months. In most instances, these referrals have led to the issuance of federal or state search warrants. Customs is also involved in joint efforts on Internet-related investigations involving money laundering and child pornography distribution with officials in countries such as Indonesia, Italy, Honduras, Thailand, and Russia.

As international issues become more prevalent in investigations of Internet-facilitated offenses, U.S. law enforcement agencies must continue to develop cooperative working relationships with their foreign counterparts. The 24/7 high-tech point-of-contact network established among the G-8 countries and others must continue to be developed and expanded to include more countries. In addition, the U.S. should continue to work with other countries, international groups, and industry to develop comprehensive and global plans for addressing the complex and challenging legal and policy issues surrounding jurisdiction raised by unlawful conduct on the Internet.

#### **IV. THE ROLE OF PUBLIC EDUCATION AND EMPOWERMENT**

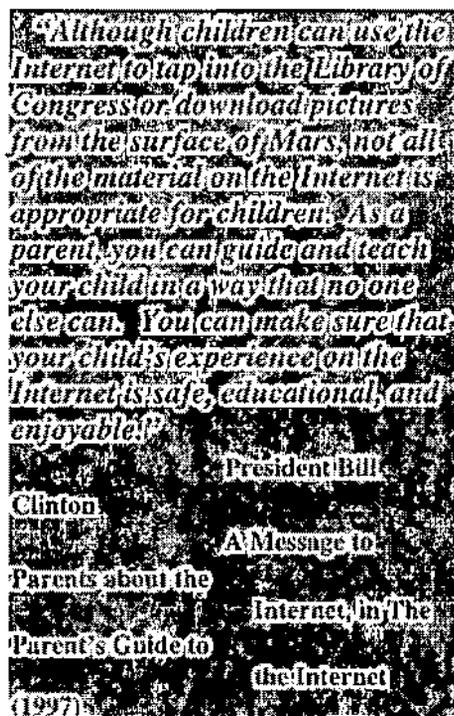
The third component of the Working Group's 3-part strategy for responding to unlawful conduct involving the use of the Internet is to implement aggressive efforts to educate and empower the public to minimize risks associated with the Internet and to use the Internet responsibly through technological and non-technological tools. Although both types of tools can be extremely useful when used appropriately, "one size does not fit all." One must weigh the advantages and disadvantages in determining which set of tools will work best for an individual's particular situation.

This part of the report therefore discusses existing and potential new tools and resources that can be used to educate and empower parents, teachers, and others to prevent or minimize the risks from unlawful conduct involving use of the Internet. First, we review the technological and non-technological tools that are available for parents and teachers to use to help ensure that children have a safe and rewarding experience online. Next, we discuss how consumers can educate themselves in order to avoid fraudulent and deceptive practices on the Internet. In particular, this part highlights how several federal agencies are using technology to educate consumers and how they are working with the private sector to develop effective consumer protection practices. Many other agencies are undertaking similar efforts. Last, we discuss government-industry cooperation efforts to educate the public on the importance of being good "cybercitizens."

##### **A. Educating and Empowering Parents, Teachers, and Children**

With the growing number of U.S. classrooms connected to the Internet and the rising number of personal computers used in the home, more and more children are now able to access the Internet. Almost 90 percent of public schools – including over 1 million classrooms – in the U.S. are connected to the Internet. Over 40 percent of American households own computers and one-quarter of all households have Internet access. 25

One of the greatest benefits of the Internet is the access it provides children to such things as educational materials, subject matter experts, online friendships, and penpals. Nevertheless, like many other pursuits that children engage in without adequate parental supervision, the Internet should also be approached with careful consideration of risks and benefits. One concern of course is that the Internet may allow children unrestricted access to inappropriate materials. Such materials may contain sexually explicit images or descriptions, advocate hate or bigotry, contain graphic violence, or promote drug use or other illegal activities. In the worst instances, children have become victims of physical molestation and harassment by providing personal information about themselves over the Internet and making contact with strangers.



To protect children from such risks, parents and teachers therefore need to empower themselves with the tools, knowledge, and resources to supervise and guide children's online experience and to teach children how to use the Internet responsibly.

### 1. Technological Tools

Technology provides tools that may assist in preventing children from accessing inappropriate materials on the Internet or divulging personal information about themselves or their families online. The most common technological tools are "blocking" and "filtering" software, as described more fully below.

#### (a) *Blocking Software*

"Blocking" software uses a "bad site" list and prevents access to those sites. The vendor of the software identifies specified categories of words or phrases that are deemed inappropriate and configures the blocking software to block sites on which the prohibited language appears. Although some vendors allow parents to customize the "bad site" list by allowing them to add or remove sites, others keep the list secret and do not permit parents to modify it.

Although such software can be a useful tool for restricting access to inappropriate websites in certain circumstances, they can also create a false sense of security, because they cannot restrict access to all inappropriate sites for children. The number of websites published each day far exceeds the ability of software companies to review the sites and categorize them for their "bad site" lists. <sup>26</sup> "Out of approximately 3 million separate websites in existence (each website may contain two or more separate webpages and the number of separate files, pages and graphics online is estimated at 330 million), only a small fraction have been reviewed, in aggregate, by child protection software companies." <sup>27</sup> Because the gap widens daily, with an estimated 160,000 new websites registered each month, "bad sites" will inevitably get through.

Another potential drawback is that most blocking software does not differentiate between the age of the users. What may be inappropriate for an eight year old, may be appropriate for a teenager. However, because most software only has one user setting to determine what should be blocked, either the teenager will be denied access to sites that are beneficial or the eight-year-old will be given access to sites that are inappropriate. In addition, in cases where software vendors do not allow parents to customize the "bad site" list, parents cannot make an informed decision on what material should be restricted. They must rely on the judgment of an unknown third party to decide what sites are acceptable for their children.

*(b) Filtering Software*

"Filtering" software blocks sites containing keywords, alone or in context with other keywords. For example, if parents wanted to restrict their child's access to sites related to drug use, the software would be configured to deny access to sites containing such words as "marijuana," "cocaine," "heroin," etc. Filtering software is available both directly and through some Internet service providers ("ISPs") such as Lycos or FamilyNet.

Filtering software can also be used to restrict access to inappropriate websites, but, like blocking software, they can be both underinclusive and overinclusive. They can, for example, filter sites that are either harmless or even desirable. With the example above, sites that promote drug rehabilitation, seeking help for a drug problem, or drug prevention would be blocked simply because they use the keywords. Another example of how filtering is over inclusive is denying access to the word "sex." While this filter would block certain sites with inappropriate sexual content, it would also block harmless sites that contained the words "sextuplets," "sexton," "Mars Exploration," among many others. In addition, some website operators have learned to bypass the filtering mechanism by misspelling the typical keywords.

Filtering software may also be used to block sites that have a particular label or rating. The content provider or a labeling service classifies the site in a particular category (e.g., "romance: no sex" or "explicit sexual activity") and the filtering software is programmed to deny access to sites with particular ratings. As with "bad sites," parents must rely on the judgment of unknown third parties to determine what is appropriate for their children. In this case, the content provider must self-label the site accurately or a labeling service must assign the appropriate label to the site. Another major drawback is that very few sites are labeled. Parents must decide whether to block or allow access to unrated sites. Blocking all unrated sites would deny access to harmless and educational material, while allowing access to all unrated sites would undoubtedly allow inappropriate material to get through.

*(c) Other Software*

Other types of software enable parents to monitor and control their children's use of the computer. For example, "monitoring and tracking" software allows parents to track how much time their children spend online, where their children go online, and how much time their children spend on the computer offline. "Outgoing filtering" software prevents children from sharing certain information with others over the Internet, such as their name, telephone number, and address. Every time the child tries to send the prohibited information to someone online, it shows up as "XXX."

## 2. Non-technological Tools

### (a) *What Parents Can Do*

One of the most effective ways of protecting children from inappropriate material on the Internet is to teach them to use the Internet responsibly. Parents play a major role in this by taking responsibility for children's online computer use. By doing so, parents can greatly minimize any potential risks of being online.

There are certain safety tips parents can follow to ensure that their children use the Internet safely. These tips include:

- never give out personal information, such as home address, school name, or telephone number, in a public message such as a chat room or bulletin board;
- do not post photographs of children on websites or news groups that are available to the public;
- never allow a child to arrange a face-to-face meeting with another computer user without parental permission;
- if a meeting is arranged, make the first one in a public place and be sure to accompany the child;
- never respond to messages that are suggestive, obscene, belligerent, threatening or make you feel uncomfortable;
- encourage children to tell you if they encounter such messages;
- report any inappropriate messages you receive immediately;
- consider keeping the computer in a room other than the child's bedroom to monitor his or her online use;
- get to know your children's online friends just as you get to know all of their other friends;
- set up specific rules for your children's online use, such as the time of day and length of time that they can be online and appropriate sites for them to visit. 30

There are many useful publications and websites for parents on this topic. For example, *The Parent's Guide to the Internet* (published by the U.S. Department of Education), *Site Seeing on the Internet: A Guide to Traveling in Cyberspace* (published by the FTC and the National Association of Attorneys General), and *The Parent's Guide to the Internet: Raising Your Family on the Information Superhighway* (by Travis West) explain the basics of the Internet, how it works, what is available online, and give guidance on how to ensure safe use of the Internet. For additional publications on responsible use of the Internet, visit [www.childrenspartnership.org](http://www.childrenspartnership.org) for a list of resources.

Likewise, there are many websites that give parents guidelines to promote safe, rewarding online experiences for children. For example:

- [www.getnetwise.org](http://www.getnetwise.org) – This website was created by 15 Internet companies as a comprehensive resource guide for parents. It includes instant access to tools representing the latest technologies that allow parents to block and filter inappropriate content, monitor the websites and chat rooms that their children visit, and set strict time limits on their children's online sessions. It also includes access to information on how to report a crime or other troubling activity online and provides a guide to quality, educational websites beneficial to children. The website also provides safety tips for online use.
- [www.americalinksup.org](http://www.americalinksup.org) – This website seeks to bring the online industry, families, teachers, librarians and other children's advocates together to ensure that children have a rewarding and educational online experience. It provides safety tips for parents and children; access to discussion groups of parents, teachers and other Internet users on critical safety issues; links to more than 700 quality websites for children reviewed and recommended by children's librarians; and information on local events where parents and children can learn about Internet basics and tools that promote rewarding online experiences.
- [www.cyberangels.org](http://www.cyberangels.org) – This website has been in existence since 1995 and is considered the largest Internet safety and education program. In addition to providing parents guidance on how to supervise their children online, it teaches children how to use the Internet safely with material geared toward them. For example, children can join Sophia's Safe Surfing Club, take a safe surfing quiz, and earn a safe surfing permit. Cyberangels also has Net Patrol teams that regularly monitor the Internet for child-crimes, cyberstalkers, and fraudulent scams and report it to law enforcement authorities. The website provides support groups for victims of stalking and harassment over the Internet and gives tips on how to document and report cyber-stalking. CyberAngels also provides links to safe sites and reviews and recommends blocking/filtering software.
- [www.parentech.org](http://www.parentech.org) – This site provides families and educators of middle school children (grades 6-8) with free resources focusing on how technology affects education, careers, and society. It includes parent and teacher guides in these three areas. For example, the parent's guide on technology and education has articles on how to help middle schoolers get the most out of learning with technology, a parent's guide to classroom technologies, and technology standards for middle schools. The teacher's guide to technology and careers includes articles on what skills are necessary for these careers and how to develop those skills at the middle school level. In addition, the site has a discussion corner where parents and educators can share ideas, concerns, and questions with each other and with experts from across the nation.
- [www.safekids.com](http://www.safekids.com) – This website contains various articles about Internet basics and online safety, guidelines for parents on how to supervise their children on the Internet, safety tips for children, and filtering/blocking software reviews. In addition, the site has links to other sites that offer Internet advice to parents and includes a link to report online crime against children.

### *(b) What Schools and Libraries Can Do*

As increasing numbers of children have access to the Internet from their schools and neighborhood libraries, we need to address the issue of how best to ensure that these children have positive, age-appropriate, educational online experiences. The Administration has taken the view that empowering parents, teachers, and librarians with a wide range of tools with which they can protect children in their community in a manner consistent with their values is ultimately the most effective approach and one that is most compatible with the First Amendment. 31

Schools and libraries are currently using a wide range of technology tools and monitoring techniques to ensure that children do not encounter inappropriate material or dangerous situations while online. These schools and libraries are determining what will work best in their particular schools and communities. Absent proof that local decision making is not working to protect our children, the federal government should not mandate a particular type of technology, such as filtering or blocking software. Rather, we should encourage "acceptable use" policies ("AUPs") by all public institutions that offer access to online resources, including the Internet. Such policies may include the use of blocking and filtering technologies, or they may involve the use of monitoring, smart cards, or codes of conduct. An AUP should, while being sensitive to local needs and concerns, offer reasonable assurances to parents that safeguards will be in place in the particular school or library setting that permit users to be empowered to have educational experiences consistent with their values.

In addition to AUPs, schools may also use "intranets" to restrict student access to inappropriate material. An intranet is a controlled computer network that uses similar software and transmission mechanisms as the Internet, but is accessible only to those who have permission to use it (an intranet is generally confined to users within an organization). These controls permit the intranet system managers to limit user access to Internet material as well as to restrict those outside the network from being able to reach it.

Schools and districts may also use Regional Technology and Education Consortia organizations ("RTECs") as a resource. Six regional consortia, funded by the Department of Education, assist and support states, districts, schools, and other educational institutions in the use of advanced technologies to improve teaching and student achievement. In helping schools and districts with planning and implementation of technology, RTECs can help schools identify Internet safety solutions that meet the schools' needs and policy preferences. In addition, RTECs also provide resources for teacher training in technology.

### *(c) Next Steps*

The Department of Justice and the Department of Education have funded a study by the National Academy of Sciences on how to protect children from inappropriate material on the Internet. This study will include a description of the risks and benefits of various tools and strategies that can be used to protect children from inappropriate material, an analysis of how the different tools and strategies can be used together, and case studies of how different communities have approached this problem. The final report is scheduled to be completed in November 2001.

In addition, in October 1998, Congress passed the Child Online Protection Act ("COPA") 32

that, among other things, established a Commission on Online Child Protection to examine the extent to which current technological tools effectively help protect children from inappropriate online content. The members of the commission were appointed last year, with the final members coming on board in October 1999, and the commission's report is due to Congress in November 2000.

Finally, the Departments of Commerce, Education, and Justice are planing a joint effort to host a roundtable discussion with industry representatives, especially those in the software industry, to discuss the benefits and limitations of existing blocking and filtering software. These discussions can lay the groundwork for future software contributions to Internet safety.

## **B. Educating and Empowering Consumers**

The electronic marketplace offers consumers unprecedented choice and around-the-clock accessibility and convenience. It gives established marketers and new entrepreneurs low-cost access to a virtually unlimited customer 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. Consumers must be confident that the goods and services offered online are fairly represented and the merchants with whom they are dealing – many of whom may be located in another part of the world – deliver their goods in a timely manner and are not engaged in illegal business practices like fraud or deception. Consumer confidence also requires that consumers have access to fair and effective redress if they are not satisfied with some aspect of the transaction.

This section highlights some of the Federal Trade Commission's initiatives to educate consumers through technology; the Department of Commerce's coordination efforts with the private sector to develop effective consumer protection practices; and the Food and Drug Administration's outreach campaign regarding medical products on the Internet. As described more fully below, the FTC has made innovative use of the Internet to educate and alert consumers about fraud and deceptive practices online, to disseminate its publications, to investigate potential violations, and to receive and respond to consumer complaints. The Department of Commerce has also worked with consumer and business representatives to develop codes of conduct for electronic commerce and mechanisms for consumer dispute resolution, redress, and enforcement. In addition, the FDA has used the Internet to educate consumers and health professionals about the possible risks of ordering prescription medications and other medical products on the Internet, and the Securities and Exchange Commission ("SEC") has likewise used the Internet to help investors avoid online securities fraud. The Postal Inspection Service posts consumer fraud prevention "tip sheets" and other fraud prevention information on its website ([www.usps.gov/postalinspectors](http://www.usps.gov/postalinspectors)). And, as part of its Internet Fraud Initiative, the Department of Justice has been active in public education and outreach efforts to prevent online fraud (e.g., establishing a website on identity theft and fraud ([www.usdoj.gov/criminal/fraud/idtheft](http://www.usdoj.gov/criminal/fraud/idtheft))), and the FBI has prepared an online Parent's Guide to Internet Safety ([www.fbi.gov](http://www.fbi.gov)).

### 1. FTC Initiatives: Using Technology to Educate Consumers

The FTC is committed to stemming fraudulent, misleading, and deceptive trade practices through actions that involve both law enforcement and education. Acting on the belief that the most effective consumer protection is education, the FTC has sought to help alert as many consumers as possible to the telltale signs of fraud, the importance of privacy in the

information age, and other critical consumer protection issues. Use of the Internet to develop and disseminate information about fraud and technology-related matters is integral to the FTC's education, deterrence, and enforcement efforts and has allowed the agency to reach vast numbers of consumers and businesses quickly, simply, and at low cost.

(a) *Fraud Prevention Information for Consumers*

More than 200 of the consumer and business publications produced by the FTC's Bureau of Consumer Protection are available on the agency's website in text and .pdf format. Indeed, the difference in the number of publications viewed online in 1996 and 1999 (140,000 versus 2.5 million page-views) tells the story of the Internet's coming of age as a mainstream medium and its importance to any large-scale dissemination effort. Those 2.5 million page views are in addition to the 6 million print publications distributed each year to organizations that disseminate them on the FTC's behalf.

(b) *Link Program*

The FTC also actively encourages "partners" – government agencies, associations, organizations, and corporations with an interest in a particular subject – to link to the FTC's website from their sites and to place banner public service announcements provided by the FTC on their sites. Links from the banners allow visitors to click through to the FTC site quickly to get the information the user is looking for exactly when they want it. Among the organizations that have helped drive traffic to the consumer information on [www.ftc.gov](http://www.ftc.gov) are the Alliance for Investor Education, the Arthritis Foundation, the American Association of Retired Persons, American Express, the Better Business Bureau, CBS, Circuit City, [motleyfool.com](http://motleyfool.com), the National Institutes of Health, the North American Securities Administrators Association, Shape Up America!, the U.S. Patent and Trademark Office, and Yahoo!.

(c) *"Sting" Pages*

Many Internet shoppers looking for weight loss products will find an attractive-looking site that trumpets NordiCaLite, a "safe and natural" way to lose weight. Three clicks into the sales pitch, the FTC seal appears, alerting consumers that the site was put up by the federal agency, that the product is a fake, and that certain words and phrases are tip offs to help them avoid most rip offs.

Too often, warning information about frauds reaches consumers after they've been scammed. For the FTC, the challenge is how to reach consumers before they fall victim to a fraudulent scheme. Knowing that many consumers use the Internet to shop for information, agency staff develop "sting" sites that mimic the characteristics of a site selling fraudulent products or services. "Metatags" embedded in the FTC websites make them accessible to consumers who are using major search engines and indexing services as they look for products, services, and business opportunities. The "sting" websites link back to the FTC's webpage, where consumers can find the practical, plain English information they need. The agency has developed 13 "sting" sites on topics ranging from health care products to scholarship services to vacation deals and investments, and feedback from the public has been overwhelmingly positive. Many visitors express appreciation – not only for the information, but also for the novel, trouble-free, and anonymous way it is offered.

#### (d) *Tutorials*

The FTC has also developed interactive puzzles and games to reinforce the concepts spelled out in its brochures, 1-page "news you can use" consumer alerts, and graphics. For example, to mark the first anniversary of the Telemarketing Sales Rule in December 1996, the FTC placed a recording of a fraudulent telemarketing call on its website and developed a quiz to test a consumer's ability to tell the difference between a legitimate call and fraudulent one. Later, the Field of Schemes investment fraud initiative included the launch of an online quiz called "Test Your Investment I.Q." A series of typical telephone misrepresentations asked consumers to define an investment offering as solid or risky and then explained the answers. As part of Project Mousetrap, which dealt with fraudulent invention promotion firms, the FTC created an activity designed to test a reader's "patent-ability": a crossword puzzle containing critical terms from the world of patents and idea promotion. And to support the first National Consumer Protection Week, an online crossword puzzle, a true-false quiz, and a word find that focused on credit terms were developed for the National Consumer Protection Weekly, a newsletter that was distributed electronically to consumer agencies, law enforcement officials, and corporations across the country.

#### (e) *Consumer.gov*

Armed with a vision of the Internet as a powerful tool for consumer education and empowerment, the FTC convened a group of five small federal agencies in 1997 to develop and launch a website that would offer 1-stop access to the array of federal consumer information. On the theory that consumers may not know one federal agency from another, the information is arranged topically. Federal agencies and consumers have responded well to [www.consumer.gov](http://www.consumer.gov). The site includes contributions from over 100 federal agencies and logs some 79,000 user sessions a month, each of which last an average of over four minutes. The site also houses special initiatives: The President's Council on Y2K Conversion asked the FTC to establish a Y2K consumer information site; the Quality Interagency Coordination Task Force requested a special site on health care quality; and the U.S. Postal Inspection Service asked that [www.consumer.gov](http://www.consumer.gov) house the site to support the "kNOw Fraud" initiative, a public-private campaign that involved sending postcards about telemarketing fraud to 115 million American households in the fall of 1999. The original [www.consumer.gov](http://www.consumer.gov) team received the Hammer Award for its efforts. The FTC continues to maintain the site.

#### (f) *Spam Mailbox*

Millions of consumers are besieged by unsolicited commercial e-mail ("UCE") or "spam" every time they open their e-mailboxes. At best, spam is annoying. At worst, it is costly and disruptive to consumers. <sup>33</sup> Hoping to relieve consumer frustration and gain a foothold on deceptive e-mail offers, the FTC invited consumers to forward their spam to a special address ([uce@ftc.gov](mailto:uce@ftc.gov)). With 3,000 e-mails arriving each day, the FTC has been able to build a spam database that is an extremely helpful resource for investigators. With partners from the Postal Inspection Service, the agency lets "junk e-mailers" know how not to break the law, and lets consumers know how to recognize the 12 most common types of e-mail fraud, known as the "dirty dozen."

#### (g) *Online Complaint Handling*

By 1998, with consumer use of the Internet to access information, entertainment, products

and services becoming routine, the FTC began accepting consumer complaints electronically. The consumer response to the online complaint feature indicates that the FTC is meeting a real need: The agency receives online – and responds online to – an estimated 1,000 complaints and inquiries a week.

#### *(h) Business Education for Online Marketers*

As part of its mission, the FTC provides guidance to online marketers on how to assure that basic consumer protection principles apply online. Many of these entrepreneurs, new to the Internet and to marketing in general, may be unfamiliar with consumer protection laws. But even experienced marketers have raised novel issues in their efforts to apply traditional consumer protection laws to the online environment. The FTC has used a variety of approaches to get its consumer protection messages out to the business community, from compliance guides, brochures and speeches at industry and academic meetings and conferences to e-mails and Web-based public service announcements, staff advisory letters on [www.ftc.gov](http://www.ftc.gov), use of the trade press to promote the availability of information on the agency site, and workshops on issues of interest and posting the transcripts.

#### *(i) Publications for Business*

Among the publications for business that have been distributed widely in print and online are *Advertising and Marketing on the Internet: Rules of the Road*, which has had a print distribution of over 22,000 and over 33,000 page-views of the online version. In addition, two business alerts – *Selling on the Internet: Prompt Delivery Rules* and *Website Woes: Avoiding Web Service Scams* – have been widely disseminated.

#### *(j) Surfs*

Just as consumers were discovering the benefits of "surfing" the Internet for instant access to information, FTC staff saw the value of surfing to educate businesses and to investigate potential legal violations. Since December 1996, when the FTC organized its first "surf" to ferret out pyramid schemes, it has become clear that this tool gives new meaning to efficiency. To date, the FTC has led some 20 surfs, with over 250 agencies and consumer protection agencies around the world, identifying some 4,000 commercial websites that make dubious claims, largely in the promotion of health and diet products, pyramid schemes, business opportunities, investments, and credit repair.

Internet surfs allow law enforcement officials to survey the nature and scope of particular violations online. They also offer an opportunity to educate website operators – many of whom are new entrepreneurs unaware of existing laws – instantly and directly. When agency staff surfers identify a site that may have problems, they send an e-mail message that explains why the site may violate the law. Their message also provides a link to the FTC website for more information and gives notice about a follow-up visit. These follow-up surfs reveal that about 20 to 70 percent of the problem sites in a particular area are improved or removed. Those sites that continue their problem practices may be subject to further investigation and enforcement.

#### *(k) Protecting Privacy Online*

In May 1998, at the request of the Vice President, the FTC used [www.consumer.gov](http://www.consumer.gov) to unveil

a 1-stop shop for information about how to protect one's privacy both on and off the Internet. The "About Privacy" site explains consumer privacy rights and provides visitors with contact information to ask that their personal information not be shared with third parties. For example, the page provides information on how to contact credit bureaus, state motor vehicle offices, and marketing organizations via the web, telephone, or mail. It includes sample opt-out letters that consumers can tailor to their own needs, as well as hyper-links to each of the three major credit reporting bureaus and the Direct Marketing Association's opt-out pages.

In addition, the FTC has initiated a major multi-pronged information campaign focused on the provisions of the recent Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506, which requires parental permission before collecting data from those under 13 years old. See Children's Online Privacy Protection Rule, 16 C.F.R. pt. 312 (1999). Businesses are being alerted to their responsibilities, and parents and youngsters are learning about their rights under the law.

## 2. Department of Commerce Initiatives

U.S. government policymakers and law enforcement officials are working to ensure consumer confidence in the virtual marketplace by enforcing existing legal protections and encouraging private sector leadership. Last spring, the Department of Commerce challenged the private sector to work with consumer representatives to develop effective consumer protection practices, including developing codes of conduct for business-to-consumer electronic commerce and alternative, easy-to-use mechanisms for consumer dispute resolution, redress, and enforcement. This approach recognizes that as e-commerce expands to encompass more international business-to-consumer transactions, alternative, easy-to-use mechanisms for consumer dispute resolution, redress and enforcement can help to ensure strong and effective consumer protection in the online environment and obviate the need for immediate resolution of the difficult issues surrounding jurisdiction and choice of law that would result if disputes had to be resolved in the courts.

There have been several significant responses to this challenge. In June 1999, the Better Business Bureau's online division, BBBOnline, announced a project to develop a Code of OnLine Business Practices (see [www.bbbonline.org](http://www.bbbonline.org)). BBBOnline will work with industry, consumer representatives and government to develop a code to provide online merchants with guidelines to implement important consumer protections, such as disclosure of sale terms, data privacy, dispute resolution mechanisms, and non-deceptive advertising.

A similar effort was initiated in August 1999 with the formation of the Electronic Commerce and Consumer Protection Group, whose members include a number of industry leaders such as America Online, American Express, AT&T, Dell, IBM, Microsoft, Time Warner Inc., and Visa. This group is committed to working with consumer leaders to address electronic commerce confidence issues by formulating concrete approaches to protect consumers and facilitate e-commerce (see [www.ecommercegroup.org](http://www.ecommercegroup.org)).

## 3. FDA's Outreach Campaign

As part of a major public education campaign, the FDA is informing consumers about the potential public health risks of buying medical products on the Internet. To increase awareness, FDA has developed a multimedia education campaign that includes messages targeted to specific audiences and the formation of partnerships for creating and disseminating

information through government agencies, national organizations, consumer groups, and the Internet industry. The campaign will include public service announcements, brochures, newspaper articles, media interviews, and an FDA website ([www.fda.gov](http://www.fda.gov)).

FDA's website on buying medical products online provides information on how consumers can protect themselves from certain online practices involving the sale of FDA-regulated products; reports on FDA's enforcement efforts; advice on spotting health care fraud; and answers to frequently asked questions about online drug sales. Consumers who suspect that a website is illegally selling human or animal drugs, medical devices, biological products, foods, dietary supplements, or cosmetics can also complete and submit to FDA an electronic complaint form provided at the site.

#### 4. SEC's Investor Education Efforts

The Securities and Exchange Commission ("SEC") believes that an educated investor is the best defense – and offense – against securities fraud. Investors who know what questions to ask and how to detect fraud will be less likely to fall prey to con-artists, on or off the Internet. And, because they are more likely to report wrongdoing to the SEC and their state securities regulators, educated investors serve as an important early warning system to help regulators fight fraud. In particular, the SEC's Internet mailbox ([help@sec.gov](mailto:help@sec.gov)) and online complaint form have made it easy and convenient for investors to express concerns and to report complaints to the agency.

The SEC publishes and distributes more than a dozen free brochures that explain in plain English how the securities industry works, how to invest wisely, and what to do if something goes wrong. They include *Internet Fraud: How to Avoid Online Investment Scams*, which helps investors identify different types of Internet fraud, describes what the SEC is doing to fight Internet investment scams, and explains how to use the Internet to invest wisely. These and other materials are available on the SEC's website ([www.sec.gov/consumer/online.htm](http://www.sec.gov/consumer/online.htm)).

Because investors increasingly use the Internet to research investment opportunities and to buy and sell securities, the SEC in 1999 launched a revised investor education page on the SEC's website ([www.sec.gov/invkhome.htm](http://www.sec.gov/invkhome.htm)). The new page features interactive quizzes and calculators, information about online investing, tips for avoiding Internet fraud, and a special section for students and teachers. The page also features the SEC's latest investor alerts, such as *Tips for Online Investing: What You Need to Know About Trading in Fast-Moving Markets* and *Day Trading: Your Dollars at Risk*. In addition to individual securities firms, a number of financial services industry associations, educational organizations, consumer groups, media outlets, and publicly traded companies provide links from their websites to the SEC's website.

#### 5. CPSC's Consumer Outreach Efforts

An important part of the mission of the Consumer Product Safety Commission ("CPSC") is to inform and to communicate with the public about consumer product safety issues. Because banned or recalled products can find their way into commerce via the Internet, it is important for consumers to have direct access to safety information. Through its web site ([www.cpsc.gov](http://www.cpsc.gov)), the CPSC educates the public about critical product safety issues; provides a secure and efficient means by which consumers can report unsafe products; and provides a medium through which manufacturers, importers and distributors of consumer products can

report substantial hazards associated with their products.

### C. Developing Cybercitizens

Children and young adults are the fastest growing group using the Internet. Helping children draw conclusions about behavior and its consequences in cyberspace is an important part of educating responsible (future) online users. Although most children are taught at an early age that it is wrong to break into a neighbor's house or read their best friend's diaries, we must also emphasize that it is equally wrong, and potentially more damaging, to break into their neighbor's computers and snoop through their computer files. Computer hacking "for fun" is a very serious problem, not only for the targets of the attacks, but also for law enforcement personnel who often have no way to determine the motivation for and the identity of the person behind the intrusion.

Educating children (and adults) about acceptable online behavior is crucial for the Internet to continue to grow as a safe and useful medium. Likewise, there is a need to educate the public on the dangers posed by cybercrimes and how harm can be reduced if people use technology responsibly. As the proliferation of low-cost computers and networks has spread information technology to every corner of society, people of all ages who use this technology must understand that along with the obvious benefits of technology comes a set of corresponding responsibilities. To this end, the Attorney General announced in April 1999 that the Department of Justice had joined with the Information Technology Association of America ("ITAA") for a partnership on a national campaign to educate and raise awareness of computer responsibility and to provide resources to empower concerned citizens.

The Cybercitizen Awareness Program seeks to engage children, young adults, and others on the basics of critical information protection and security and on the limits of acceptable online behavior. The objectives of the program are to give children:

- An understanding of cyberspace benefits and responsibilities;
- An awareness of potential negative consequences resulting from the misuse of the medium;
- An understanding of the personal dangers that exist on the Internet and techniques to avoid being harmed; and
- An ability to commit to adhere to these principles as they mature.

Thus far, the campaign has received \$300,000 in grants from the Department of Justice's Office of Justice Programs. The partnership awarded a contract to a public relations firm in December 1999 to implement the objectives of the campaign. The Department of Justice and ITAA believe that the program will play a significant role in deterring potential hacking, educating the public about the potential dangers of the Internet, raising awareness about the potential consequences of online activities, reducing the threat to the nation's critical infrastructure, increasing online security in the United States, and providing savings to information technology resources owners and users who suffer economic losses as a result of computer crimes.

In addition to the awareness program detailed above, the Cybercitizen Partnership also has initiated a personnel exchange program between private business and federal agencies that is designed to educate both groups about how the other responds to threats and crimes over the Internet. This initiative will allow companies to find out how best to help law-enforcement agencies, and government officials will learn what business interests and influences drive industry decisions. The exchange program will be coordinated by the ITAA, which intends to detail personnel from the private sector to the FBI's National Infrastructure Protection Center. The partnership also expects to create a directory of computer experts and computer security resources so that law enforcement will know where to turn when they need assistance from industry.

## V. CONCLUSIONS AND RECOMMENDATIONS

Ensuring the safety and security of those who use the Internet is a critical element of the Administration's overall policy regarding the Internet and electronic commerce, a policy that seeks to promote private sector leadership, technology-neutral laws and regulation, and an appreciation of the Internet as an important medium for commerce and communication both domestically and internationally

Consistent with the Administration's overall policy, the Working Group recommends a 3-part approach for addressing unlawful conduct on the Internet:

- First, any regulation of unlawful conduct involving the use of the Internet should be analyzed through a policy framework that ensures that online conduct is treated in a manner consistent with the way offline conduct is treated, in a technology-neutral manner, and in a manner that accounts for other important societal interests such as privacy and protection of civil liberties;
- Second, law enforcement needs and challenges posed by the Internet should be recognized as significant, particularly in the areas of resources, training, and the need for new investigative tools and capabilities, coordination with and among federal, state, and local law enforcement agencies, and coordination with and among our international counterparts; and
- Third, there should be continued support for private sector leadership and the development of methods – such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts – that educate and empower Internet users to prevent and minimize the risks of unlawful activity.

The challenges to the federal government of unlawful conduct involving the use of the Internet are many. On one hand, the Internet offers unparalleled opportunities for socially beneficial endeavors. At the same time, individuals who wish to use a computer as a tool to facilitate unlawful activity may find that the Internet provides a vast, inexpensive, and potentially anonymous way to commit unlawful acts, such as fraud, the sale or distribution of child pornography, the sale of guns or drugs or other regulated substances without regulatory protections, and the unlawful distribution of computer software or other creative material protected by intellectual property rights.

In its analysis of existing federal laws, the Working Group finds that existing substantive federal laws generally do not distinguish between unlawful conduct committed through the

use of the Internet and the same conduct committed through the use of other, more traditional means of communication. To the extent these existing laws adequately address unlawful conduct in the offline world, they should, for the most part, adequately cover unlawful conduct on the Internet. There may be a few instances, however, where relevant federal laws need to be amended to better reflect the realities of new technologies, such as the Internet.

Despite the general adequacy of laws that define the substance of criminal and other offenses, however, the Working Group finds that the Internet presents new and significant investigatory challenges for law enforcement at all levels. These challenges include the need for real-time tracing of Internet communications across traditional jurisdictional boundaries, both domestically and internationally; the need to track down sophisticated users who commit unlawful acts on the Internet while hiding their identities; the need for hand-in-glove coordination among various law enforcement agencies; and the need for trained and well-equipped personnel – at federal, state, local, and international levels – to gather evidence, investigate, and prosecute these cases. In some instances, federal procedural and evidentiary laws may need to be amended to better enable law enforcement to meet these challenges.

Indeed, the Working Group concludes that the federal government must continue to devote further attention to these important challenges. The report contains specific suggestions on areas on which additional resources and further evaluation are needed. These recommendations recognize that there are no easy answers to the challenges posed by unlawful conduct on the Internet. At the very least, however, significant attention should be given to the issues, and open dialogue and partnerships among law enforcement agencies, industry, and the public must continue.

In light of its mandate, the Working Group confined its analysis to existing federal laws. A logical next step would be an expanded analysis of state (and, to the extent relevant, local) laws that focuses on whether those laws are adequate to investigate and prosecute unlawful conduct on the Internet. Because coordination and cooperation among federal, state, and local law enforcement agencies are key to our efforts to prevent, deter, investigate, and prosecute such unlawful conduct, such an analysis would provide states and others with a blueprint for translating the conclusions in this report into a more comprehensive approach to meeting the substantial challenges presented.

Finally, an essential component of the Working Group's strategy is continued support for private sector leadership, industry self-regulation, and the development of methods – such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts – that educate and empower Internet users so as to prevent and minimize the risks of unlawful activity. This Administration has already initiated numerous efforts to educate consumers, parents, teachers, and children about ways to ensure safe and enjoyable Internet experiences, and those efforts should continue. The private sector has also undertaken substantial self-regulatory efforts – such as voluntary codes of conduct and appropriate cooperation with law enforcement – that show responsible leadership in preventing and minimizing the risks of unlawful conduct on the Internet. Those efforts must also continue to grow. Working together, we can ensure that the Internet and its benefits will continue to grow and flourish in the years and decades to come.

---

<sup>1</sup> See Towards Digital eQuality (1999) (Second Annual Report of the U.S. Government Working Group on Electronic Commerce) <<http://www.ecommerce.gov/annrpt.htm>>; A Framework for Global Economic Commerce (1997) <<http://www.ecommerce.gov/framework.htm>>.

2 The "Internet" has been defined as "collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected worldwide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio." Internet Tax Freedom Act, Pub. L. No. 105-277, Div. C, tit. 11, § 1101(e)(3)(C); Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, Div. C, tit. 13, § 1302(6). Internet connections are made using the same kinds of lines, cables, and satellites as those that join telephones. Unlike traditional telephone calls, however, which transmit information by circuit-switching (i.e., the use of a dedicated circuit between a caller and a call recipient, much like the string between two cans), the Internet transmits information by packet-switching. In packet-switching, communications are broken into small pieces, and each piece is placed into a packet. Each packet is sent individually to the recipient, with packets arriving at their destination through different routes. The communication is then reconstructed at the receiver's end.

3 Internet Users Now Exceed 100 Million, N.Y. Times, Nov. 12, 1999, at C8.

4 Forrester Research, U.S. Online Business Trade will Soar to \$1.3 Trillion by 2003 (visited Dec. 17, 1998) <<http://www.forrester.com>>.

5 Cf. 1999 CSI/FBI Computer Crime and Security Survey, 5 Comp. Security Iss. & Trends 1 (Winter 1999) (discussing results of voluntary, anonymous survey of computer security breaches and noting uncertainties). Truly reliable estimates of computer crime are not currently available, because (1) there is no commonly accepted definition of a computer crime; thus, it is unclear whether certain criminal activity should be included, or excluded, from computer crime statistics; (2) for a variety of reasons discussed in this report, most computer crimes are still not detected or reported; and (3) even when such crimes are reported, they are not reported to any central authority for compilation.

6 For example, in November 1999, an Internet bookseller, which also operated an Internet communications service that provided e-mail service to its book-dealer customers, was charged with intercepting its customers' electronic communications and possessing, without authorization, customer password files with intent to defraud. During a 6-month period in 1998, the bookseller was alleged to have intercepted e-mail messages from its dealers to Amazon.com in an attempt to gain a competitive commercial advantage for its own book-selling business by compiling a database of dealer purchases and by gathering information to analyze the book-selling market. The bookseller intercepted and copied thousands of e-mail communications to which it was not a party and was not entitled. As a result of this prosecution, the bookseller agreed to pay a \$250,000 fine as part of a plea agreement.

7 In addition, safety nets created by existing regulatory systems to protect consumers from unlawful conduct in the offline world should be examined for their ability to protect consumers from unlawful conduct in the online world.

8 "Cross-site scripting" is a serious problem that hides computer code in links to popular Internet sites and is not limited to software created by a particular company or a particular web browser. Private sector cooperation and awareness are vital to protecting consumers against this potential exploit. Recognizing this, many private-sector leaders are educating consumers and Internet businesses about the "cross-site scripting" problem. Indeed, several computer companies published information on their websites regarding the exploit and its hazards within a day after the warning was issued.

9 For example, though beyond the scope of this report, the increasingly global nature of e-commerce can raise law enforcement issues in the areas of tax evasion, see 26 U.S.C. § 7201; tax fraud, see id. § 7206(1); and money laundering, see 18 U.S.C. § 1956. The use of offshore foreign trusts and the ability to move assets electronically and to conduct financial transactions over the Internet can place information beyond the reach of criminal investigators. Emerging technologies, such as cyberbanking, stored value cards, and Internet brokerages can also be used to facilitate the hiding of assets from U.S. taxing authorities or placing them beyond their reach.

10 The distribution of hate speech, for example, raises particularly difficult policy questions. Germany, in light of its history, prohibits neo-Nazi speech and the distribution of hate literature. But Germans and others now complain not only that neo-Nazi speech itself is suddenly accessible throughout Germany via the Internet, but also

that hate literature and similar materials are sent or made available via the Internet to customers in Germany from other countries, including from U.S.-based websites.

11 Technological solutions will, of course, play an important role in how the issue of online identification evolves and is resolved. Industry continues to develop new technological methods for verifying the identity of individuals, such as digital signature protocols and biometric technologies, but the full range of these technologies has not yet been fully perfected. As these new technologies emerge and grow, they should be evaluated for their benefits, as well as their limitations, for law enforcement and online commerce.

12 For further discussion of the availability of bombmaking information on and off the Internet, see U.S. Dep't of Justice, *Report on the Availability of Bombmaking Information, the Extent to Which Its Dissemination Is Controlled by Existing Law, and the Extent to Which Such Dissemination May Be Subject to Regulation Consistent with the First Amendment to the United States Constitution (1997)* (report submitted to the U.S. House of Representatives and the U.S. Senate pursuant to section 709(a) of the Antiterrorism and Effective Death Penalty Act of 1996) <[www.usdoj.gov/criminal/cybercrime/bombmakinginfo.htm](http://www.usdoj.gov/criminal/cybercrime/bombmakinginfo.htm)>.

13 Coordination among law enforcement, intelligence, and defense agencies is particularly important, because the origin and motive of a cyberattack can be difficult to ascertain, at least at the outset of an attack. The government agency with responsibility for responding to a cyberattack, and the nature of the response, is likely to turn on the particular circumstances of the attack.

14 These efforts may include, for instance, technological solutions, information-sharing arrangements, appropriate monitoring or other system security mechanisms, the timely reporting of potential intrusions or other cybercrimes, and educational and other outreach efforts.

15 Russian KGB agents were apparently paying the hacker, sometimes using cocaine as currency, to gather information on the United States's "star wars" missile defense program. Stoll's 10-month odyssey in search of the hacker is recounted in his book, *The Cuckoo's Egg: Tracking A Spy Through The Maze of Computer Espionage* (1989).

16 See Remarks of the Honorable Janet Reno, Attorney General of the United States, to the National Association of Attorneys General (Jan. 10, 2000) <[www.usdoj.gov/ag/speeches/2000/011000naagfinalspeech.htm](http://www.usdoj.gov/ag/speeches/2000/011000naagfinalspeech.htm)>.

17 An example of an industry practice that leaves carriers without critical data is the generation and maintenance of records for local telephone calls. In the past, most Americans received an itemized list of all of their local telephone calls (i.e., calls within their area code or state) with their monthly telephone bill. But as telephone companies moved to bulk or flat-rate billing for local calls, there was no longer a revenue-based reason to list this information in phone bills and, indeed, to collect the information at all. As a result, when law enforcement needs records to confirm that a suspect dialed an ISP from his or her home (a local telephone call), that information will not exist if it was never collected in the first place.

18 Some countries require by law that data routinely be retained, while other countries explicitly prohibit such retention. A third sub-set of countries leave it to the marketplace to determine what should be retained.

19 See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. 31 (L 281); Directive 97/66/EC of the European Parliament and of the Council of December 15, 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, O.J. 1 (L 24) (Jan. 30, 1998). See generally Peter Swire & Robert Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (1998).

20 Because advertising revenue for a website is often tied to the level of visitor traffic, website operators often offer free e-mail accounts as a way of increasing their customer base.

21 Gary H. Anthes, "Stealth E-mail" Poses Corporate Security Risk, *Computer World*, Feb. 12, 1996, at 1A

(available at 1996 WL 2371156).

22 For example, an unsophisticated computer user may believe that he has deleted files containing child pornography when, in fact, that evidence is still on the computer and can be retrieved by a computer forensics expert. At the same time, however, a sophisticated computer user could "hide" evidence on a computer that is inaccessible to a law enforcement forensics expert. There have also been cases where computer users have "booby-trapped" evidence on a computer so that if a particular file is accessed, it is destroyed or made incomprehensible.

23 The San Diego Regional Computer Forensics Laboratory, which provides computer forensic analysis and support to the law enforcement community in Southern California, is a joint project among 32 federal, state, and local law enforcement agencies. It is staffed by 16 computer forensic examiners and a lab director. All of the personnel are detailed from their parent agencies and departments, most on a full-time basis. They represent five federal agencies and seven non-federal police agencies. Thirteen of the 15 staff members (11 non-FBI) have been trained by the FBI's Computer Analysis and Response Team ("CART"). The remaining three have received substantial training through their agencies. The lab has received substantial financial support from the California Border Alliance Group and has been provided space and resources by the FBI. More information about the lab can be found at <http://www.usdoj.gov/usao/cas/sdlab.htm>.

24 See generally U.S. Dep't of Justice, The National Information Infrastructure Protection Act of 1996: A Legislative Analysis (1996) <[http://www.usdoj.gov/criminal/cybercrime/1030\\_anal.html](http://www.usdoj.gov/criminal/cybercrime/1030_anal.html)>.

25 See U.S. Dep't of Commerce, Falling Through the Net: Defining the Digital Divide (July 1999).

26 Parry Aftab, Parents' Guide to the Internet: And How to Protect Your Children in Cyberspace (1998).

27 *Id.*

28 *Id.*

29 *Id.*

30 Lawrence J. Magid, Child Safety on the Information Highway (1998) <[http://www.safekids.com/child\\_safety](http://www.safekids.com/child_safety)>.

31 See Letter from Assistant Secretary of Commerce Larry Irving to Federal Communications Commission Chairman William E. Kennard (Apr. 7, 1999) (encouraging acceptable use policies for public institutions offering access to the Internet).

32 COPA restricts the dissemination of "obscene" materials and materials "harmful to minors" over the world wide web. See 47 U.S.C. § 231. 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 *id.* § 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 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).

33 Several bills were introduced in the most recent session of Congress to regulate and limit spam. For instance, Senator Murkowski's Inbox Privacy Act, S. 759, 106th Cong. (1999), would require junk e-mailers to include identifying data and explicit opt-out provisions in their messages and to comply with recipient requests to cease spamming them. S. 759 would also prohibit junk e-mailers from sending spam to any domain with a no-spamming policy. Congressman Miller's Can Spam Act, H.R. 2162, 106th Cong. (1999), would permit ISPs to sue those who violate their anti-spam policies and would establish criminal penalties for falsifying a domain name on spam.

- 
- [Appendices to "The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet \(March 9, 2000\)](#)
  - [More Information on: Prosecuting Crimes Facilitated by Computers and by the Internet](#)
  - [More information on: Electronic Commerce](#)

Go to . . . [CCIPS Home Page](#) || [Justice Department Home Page](#)

---

*Last updated April 4, 2000*  
usdoj-crm/mis/mdf

---