COMPUTER CRIME

A JOINT REPORT

State of New Jersey

Commission of Investigation

Attorney General

of New Jersey

JUNE 2000

COMPUTER CRIME

A JOINT REPORT

State of New Jersey

Commission of Investigation

Attorney General

of New Jersey

LESLIE Z. CELENTANO
CHAIR

JOHN J. FARMER, JR.

M. KAREN THOMPSON
W. CARY EDWARDS
AUDRIANN KERNAN
COMMISSIONERS

JUNE 2000

The Report, complete with hypertext links, is available on the Commission's Web site at www.state.nj.us/sci

COMPUTER CRIME

TABLE OF CONTENTS

COMPUTER CRIME

INTRODUCTION

In an unprecedented joint project, the State Commission of Investigation (hereinafter “Commission” or “SCI”) and then-Attorney General Peter G. Verniero held three days of public hearings on computer crime on February 23, 24 and 25, 1999. The hearings, with more than 30 expert witnesses, capped extensive inquiries by the Commission and the Attorney General’s Office, headed since June 1999 by Attorney General John J. Farmer, Jr. They underscored the need for law enforcement at all levels to coordinate efforts to control the “dark side” of the computer revolution. This includes prosecuting high-tech conduct offending criminal laws, pursuing civil remedies for online wrongdoing, and helping adults and children to protect themselves in cyberspace.

Computer technology and communication confer obvious advantages on businesses, governments, schools and individuals. With nominal resources, people and institutions can, via computers, leap state and national boundaries to explore vast stores of information and benefit from innumerable commercial opportunities. However, Commission Chair Leslie Z. Celentano cautioned in her public hearing opening remarks that “[as] on any frontier, … predatory elements seek to take advantage of those reaching for new opportunities.” With proper safeguards, adults and children should be able to enjoy and profit from cyberspace — sometimes called the “digital highway” or the “information superhighway” — without falling prey to schemers, predators and intruders.

According to the U.S. Department of Commerce, 40 percent of American households owned personal computers at the end of 1998. A quarter of those had access to the Internet, a global group of interconnected computer networks, communications equipment and software. The Internet furnishes nearly 200 million worldwide users access to measureless riches of information and services. According to Forrester Research, Inc., which tracks Internet commerce, total U.S. business trade on the Internet reached $43 billion in 1998 and is projected to rise to $1.4 trillion in 2004. Spending on Internet auction sites alone totaled $1.4 billion in 1998 and is predicted to grow to $19 billion by 2003.

While each of the networks that make up the Internet is owned by a public or private organization, no single organization or government owns or controls the Internet. Originally created to further defense, scientific and academic endeavors, the Internet, which also affords

users the ability to communicate via electronic mail (“e-mail”), grew slowly but steadily until 1994. At that time, the World Wide Web (“the Web”), the graphical user interface to the Internet, was introduced.

The Web prompted extraordinary growth in both the size and the use of the Internet. Once limited to military and educational undertakings, the Web has expanded to become an integral and even essential part of vast numbers of businesses and households. It consists of millions of electronic “storefronts,” or repositories, called Web sites. Businesses, organizations, government agencies and individuals set up Web sites, which may be a combination of text, graphics, still pictures, videos and sounds. Each Web site has an Internet address called a uniform resource locator (URL).

When it became clear that they could facilitate business-to-business and consumer-to-business electronic commerce (“e-commerce”), the Internet and the Web rocketed to importance in the economy. Online businesses now abound, and credit card purchases over the Internet occur 24-hours-a-day.

Befitting the vastness of cyberspace, which includes the Internet, computer-related crimes impacting New Jersey are varied and extensive. Child pornographers and pedophiles entice and exploit children via the Internet. Extremists and hate groups take advantage of high technology to rend society and foster bias-related crime. Unscrupulous individuals intrude upon supposedly secure computers and databases releasing catastrophic computer viruses and engaging in industrial espionage. Swindlers in cyberspace undermine confidence in e-commerce. With the aid of fly-by-night Web sites, identity thieves glean personal information in order to enrich themselves at the expense of their victims’ creditworthiness and reputations. Unregulated Internet gambling operations dupe the unwary. Lastly, high technology helps criminals foil law enforcement’s efforts to detect and prosecute a host of traditional crimes.

Apart from the breadth of potential misconduct, the unique nature of the Internet presents challenges not evident in the traditional law enforcement milieu. Enforcers must overcome problems involving jurisdiction, evidence access and preservation, applicability of current laws, vulnerability of a virtually unlimited victim pool, and practical obstacles to the identification of perpetrators.

The Attorney General’s Internet Working Group was established in 1997 and charged with coordinating the extensive high-technology resources of the Department of Law and Public Safety in order to enhance the ability of the State’s law enforcement community to address Internet and advanced technology issues. The Internet Working Group meets monthly to design strategies for handling computer-related public safety issues, including: child endangerment, threats and stalking, bias crimes, identity theft, online gaming, sale of drugs

and other illegal products, Consumer Fraud Act violations and discriminatory practices. The Internet Working Group also advises the Attorney General on matters concerning Internet legislation and policy. Training is another important focus of the Internet Working Group. Through the Department's divisions, the Internet Working Group ensures that law enforcement agencies throughout the State are advised of emerging high technology crimes and trained in methods to investigate and prosecute these crimes.

The Internet Working Group is in the process of constructing a Web site that will provide information to the public about safe computing practices and the proper methods for reporting high technology crimes. The Web site will integrate information from a variety of sources, to provide a single resource where individuals and education, civic and business groups can keep abreast of developing computer crime issues.

If an emergency or complex criminal matter requires it, the Working Group can coordinate the State's response. The Computer Analysis and Technology Unit (CATU) in the Division of Criminal Justice, the High Technology Crime and Investigations Support Unit (HTC&ISU) in the Division of State Police, prosecutors' office personnel specializing in computer crime control, and the E-Commerce Investigative Unit in the Division of Consumer Affairs are directly involved in the effort. The Statewide Computer Crime Task Force utilizes the combined assets of the HTC&ISU and the CATU. It includes representatives of federal law enforcement as well as county prosecutors' offices and municipal police departments. The task force is designing and implementing a training program for deputy attorneys general and assistant prosecutors in the area of computers, computer forensics, the Internet and the legal issues associated with the investigation, presentation and admissibility of digital and electronic evidence. The task force is proactive in disrupting computer crime activities within the New Jersey area by identifying, investigating, arresting and prosecuting individuals responsible for violating the criminal statutes.

Although we conclude this report with several recommendations to strengthen society's ability to fight computer-related crime, no amount of law enforcement can safeguard computer users better than their informed precautions. Therefore, the report comprehensively details lessons learned during the joint project and refers readers to many helpful institutions, programs and individuals. In this way, we expect to assist citizens, as well as their public officials.

This report contains a variety of links to Web sites and references to resources available through government, nonprofit and commercial entities. Hypertext links are available in the copy of the report found at the Commission's Web site (www.state.nj.us/sci). The links and references are provided solely for informational purposes.

Their inclusion does not constitute endorsement. References to testimony in the report pertain to witnesses testifying at the February 1999 public hearing.

CHILDREN IN JEOPARDY

THE PROBLEM

It has been estimated that 11—15 million children in the United States are currently online. Industry experts estimate that the number will rise to 45 million by the year 2002. Through Urban League community centers, free public libraries, Newark's Millennium Project and like programs, poor children will achieve online experience comparable to those whose families can afford computers at home. More and more "latchkey kids" in empty houses or participants in after school programs will shun passive television and gravitate toward the Internet, where they can interact with other children and adults.

Children use cyberspace to talk with friends, complete homework assignments, and explore museums, libraries and universities. While providing almost limitless opportunities to learn, this "information age" has exposed children to supercharged versions of the old threats of child molestation and child pornography. Child molesters and pornographers take full advantage of Internet service providers (ISPs), Internet relay chat (IRC) (hundreds of thousands of electronic "chat rooms" where users can "talk" to others by typing on their keyboards), and the Usenet (tens of thousands of bulletin board-style discussion groups, often called "newsgroups"). These provide to such predators abundant hunting grounds in which to find young victims. Moreover, at nominal expense, and regardless of where they reside in the world, they can, and do, readily view and trade or sell pictures and movies of young or very young children being sexually molested by adults, snuff erotica (real murder done for sexual arousal), bestiality and the like.

IRC channels are similar to the chat rooms offered by ISPs, such as America Online, but they are not proprietary and thus not subject to any policing mechanisms ISPs often have in place. IRC channels are accessible to anyone with an Internet connection and the necessary free software ("shareware"). The users of these channels can communicate in "real-time"; that is, they are able to type messages that are seen by others instantly. They may convey their messages to all of the other users on the channel, or they may communicate privately one-to-one. They also may send and receive contraband files, such as videos or photographs.

One significant difference between IRC channels and ISP chat rooms is that subscribers to the latter have unique and traceable screen names assigned to them. IRC channel users can assume any screen name they want and change it at any time. This makes identifying and tracking IRC users more difficult, but not impossible.

While newsgroups on the Usenet are great sources of information on virtually any subject, they are, unfortunately, used by some as a medium for distributing child pornography and for advertising services involving the exploitation of children. Users' messages are stored and made available for many other people to read. A user may access and read all of the messages other people have posted. Contrary to common misconception, individuals who post illegal material to the Usenet discussion groups may indeed be traced, arrested and convicted. People who download child pornography from newsgroups may be traced, but not as easily as those who post such material. Some system administrators occasionally notice the downloading of files with unusual names and notify law enforcement.

Some ISPs merely give their customers access to the Internet. Others are also online service providers that make services, such as "chat" areas, available to their members only. These "rooms" are created by the ISP's members themselves and cater to their private interests, which sometimes extend to child erotica. Although the terms of service (TOS) between ISPs and their customers often prohibit vulgar and sexually explicit room and screen names, such rooms flourish. Established ISPs, such as America Online, employ many techniques to enforce their TOSs, including account termination for accumulated violations. Currently, however, only a very small percentage of the child pornographers reported to ISP authorities have their accounts terminated. Even those who are terminated can switch to other ISPs. Their activities are not curtailed significantly until they are reported to capable, well-staffed law enforcement agencies that cooperate with one another across jurisdictional boundaries.

Producers, purveyors and consumers of child pornography cause great harm to children. As many as 70% of convicted child molesters also collect child pornography. Since the advent of video technology and digital photography, copious illicit images may be traded or sold instantaneously. Moreover, digital images do not lose quality through copying. Thus, enormous quantities of high-grade child smut are available for rapid and widespread distribution.

So-called "cyber-stalkers" or "travelers" are nothing more than child molesters seeking to have sex with the children they contact online. Eugene J. (Gene) Weinschenk, former Director of the United States Customs Service's CyberSmuggling Center, has reported that 75% of registered sex offenders routinely "surf" the Internet. Children exploited and victimized by cyber-stalkers often join the woeful ranks of the missing or abducted.

Child sexual abusers are rapidly turning the Internet and commercial online services into red-light districts, where they can distribute vast quantities of pornography — often depicting bondage and other forms of violence, including murder — and organize with like-minded individuals. The Internet gives child molesters and pornographers unprecedented opportunities to target and recruit new victims. It allows sexual predators to stalk juvenile victims anonymously from the comfort of their homes.

The Internet provides child molesters with a cloak of secrecy. Known solely by their computer code names, they pretend to be the same age as their victims. Parents, who would hustle their children away from such people at a playground, sometimes learn after it is too late that they have been their children's "bedroom buddies" via home computers. Predators can stalk children in their homes, schools and libraries without having to appear physically at those places. In this way, Internet-based child sexual exploitation can be a "silent" crime. Parents often first learn of such activity when a child tells of molestation or disappears.

Mr. Weinschenk described a distressing scenario:

> The example that I always like to use is … a little 10 or 11-year-old boy will come in [to a chat room] and say, "My mom, she won't let me get a Sony Play Station." The predator sits there and makes these notes. He'll wait awhile, try to figure out where the child is. The kids will say what school they go to, what town — eventually it will all come out.
>
> If I'm the predator, if I'm 54-year-old Gene, I'll go back in as 11-year-old Tommy and I'll say, "You know what, my mom won't let me buy it either." And 11-year-old Tommy will say, "I have an Uncle Gene, and he's going to take me out Saturday to the mall and buy me a Play Station because he thinks I should have one. He'll buy one for you too. Why don't you meet us at the mall." They're on their way.
>
> They show up at the mall … in front of Toys-R-Us. "Hey, I'm Gene. Tommy is down in the store, you know, over in Macy's somewhere. He said for me to buy this for you" and go in and buy him the Play Station. They'll go in the car …. [Fifty-four] bucks or whatever the Play Station [cost] and he's got the child. Whether or not the child is ever seen again, that's another story.

The anonymity of Internet communications can work to the advantage of law enforcers as well as predators. A trafficker in child pornography, for example, could think he is talking to a child when he really is talking to a detective. But sophisticated traffickers counter such operations by screening out undercover detectives

pretending to be pornography dealers. Such traffickers insist that their contacts forward child pornography before replying with their own material. Since authorities will not release illicit images into cyberspace, sophisticated traffickers can fend off undercover sting operations.

Would-be molesters also bide their time to foil investigators. They may monitor a “kids-only” chat room, not saying anything that would get them into trouble. They then select certain children for a “buddy list,” which reveals when designated individuals are online. Later, when an intended victim goes online, the predator can send her a direct instant message that bypasses e-mail. Thus, even parents overseeing a child’s e-mail may not be aware of dangerous communication.

National statistics on Internet sex crimes are scarce, but officials believe such crimes are numerous and increasing. The Justice Department cannot say how many crimes against children occur over the Internet because it does not break out those figures from overall statistics. However, the number of all child pornography cases filed in federal court increased by 129% in 1996. William Megary, then-Special Agent in Charge of the FBI’s Newark Division, testified, “I can say with certainty that the number of predators that are out there clearly exceeds the ability of law enforcement to address them, without question.” The *Crime Control Digest* reported in August 1999 that since January 1998 the U.S. Customs Service, the U.S. Postal Inspection Service and the FBI had made over 460 arrests involving the exchange of child pornography on the Internet.

Mr. Weinschenk testified that child pornography, traditionally restricted to bartering, is rapidly becoming a “very profitable” cottage industry. He cited a Customs Service arrest about two years ago “where people were making $25,000 a day showing CD-ROMs of child pornography.” In May 1999, U.S. Customs Commissioner Raymond Kelly reported that 95% of child pornography that comes into the United States from abroad now arrives via the Internet.

On September 1, 1998, in a stunning example of what can be achieved by worldwide law enforcement cooperation, authorities coordinated raids targeting 180 child-pornography traders in 14 countries. The raids, assisted by the CyberSmuggling Center, resulted in more than 40 arrests. Four of the original 14 arrested in the United States committed suicide. The rest were prosecuted in federal court. Authorities had targeted "wOnderland," the largest, most sophisticated online child pornography ring yet discovered. The project was called "Operation Cheshire Cat" in the United States and "Operation Cathedral" in the United Kingdom. The members of wOnderland included a resident of West Orange, New Jersey. Three United States members were women. In order to be admitted to the club, a prospective

member had to have at least 10,000 pornographic images of children on his or her computer.

WOnderland existed in Internet relay chat, where people can communicate and exchange files anonymously. For less than $100 per month, wOnderland members could buy access to the club. They then could go online, enter a private chat room and agree to exchange photos. The photos were encrypted with codes from the former Soviet KGB to prevent outsiders from gaining access to them. To join the club, potential members needed current members to vouch for them.

On October 28, 1998, 13 people and 2 Internet service providers were arrested for involvement with a group called Pedo University. Participants on three continents called themselves "faculty members" and, in newsgroups, swapped images of children having sex. One of those arrested was a 67-year-old Bridgewater, New Jersey, man calling himself "MRPERFECT" and using the computer screen name "lovable." He was arrested on state charges of endangering the welfare of a child.

Mr. Megary related a recent case involving two offenders who were arrested after molesting a 12-year-old boy:

> When a federal search warrant was executed at the suspects' residence, investigators found four computer systems, one laptop computer, a network server, four printers, a CD-ROM recording system, a digital camera and two video camcorders. More than 1,700 computer diskettes and recordable CD-ROMs were also recovered, as well as a number of used computer hard drives, videocassettes, and numerous printed photographs. It was determined that the subjects were videotaping their victims, converting the images to CD-ROMS, and distributing them on the Internet.

A notorious New Jersey case illustrates the catastrophic consequences that can flow from Internet child sexual exploitation. Last year, a teenager pled guilty to the September 27, 1997 slaying of 11-year-old Eddie Werner, who had been selling candy door-to-door in central New Jersey for a school fund-raiser. At the time of the killing, the victim's slayer was 15 years old. A 45-year-old Long Island man pled guilty on July 22, 1999 to sexually molesting the young killer in New Jersey after meeting the then-14-year-old in an Internet chat room in 1996.

State and local authorities continue to uncover instances of adults using the Internet to set up sexual encounters with children. In January 2000, four New Jersey men were arrested for allegedly arranging such meetings with 13-year-old boys and girls. The "victims" were part of a sting set up by law enforcement officials from Ocean and Monmouth counties, the State Police and the Wall and Dover

Township police departments. The officials responded to a parent's complaint that an adult had propositioned her minor son online.

The Internet also facilitates child sex tourism, which is arranged by certain miscreant travel agencies. The resulting seductions and assaults are recorded digitally, and images are shared with other sexual predators worldwide. Mr. Weinschenk testified, "There are whole groups that are dedicated to having sex with children or trading pictures or images of sex with children under three, under five." In recent years, some 25 countries, including the United States, France and Germany, have adopted laws allowing prosecution in their home countries of people accused of having sex with minors abroad.

THE MAKING OF PREDATORS: CYBERSPACE HELPS PEDOPHILES ACT OUT THEIR PERVERSION

Not all persons with pedophilia are child molesters, but the ones who are almost always collect child pornography. Many pedophiles are law-abiding citizens who have a sexual attraction towards children but control their desires and lead normal lives. Others act on their impulses, with devastating consequences for the children they encounter.

Authorities must wait for pedophiles to act before they can isolate them from society. Experts report that the average child-molesting pedophile abuses 35 children before getting caught. Many compulsively and systematically save collected child pornography to validate their actions, or as mementos and souvenirs. When sharing these treasured keepsakes, they gain strong reinforcement from like-minded persons.

The North American Man/Boy Love Association (NAMBLA), established in Boston in 1978, advocates abolishing the age of consent in sexual relations. Its members contend that it is not wrong for adults to have sex with children. Indeed, NAMBLA members profess that when they cajole children into sex, they enrich the youngsters' lives.

Active pedophiles attempt to project a benign image to their victims. They try to separate children from adults who might protect them. They ask the children to recruit others and advise them not to tell their parents about any communication or rendezvous. They use pornography to lower children's inhibitions and to blackmail them into keeping silent about the abuse.

The Internet allows child sexual predators to validate each other's degenerate behavior in pedophilia chat rooms and Web sites. Parry Aftab, Executive Director of Cyber Angels and a New Jersey lawyer, testified that her organization and Safeguarding Our Children

— United Mothers (SOC-UM) documented 17,000 Web sites on the Internet devoted to child pornography and pedophilia. By May 14, 1999, the number had jumped to 21,317, an increase of more than 4,300 sites — more than 25 percent in less than four months. The Pedophile Liberation Front (PLF) encourages the creation of Web sites devoted to sex between adults and children, and it wants children to have access to them. The National Center for Missing and Exploited Children estimates that there are about 10,000 Web sites maintained by computer pedophiles.

However many such sites exist, they are like drops in the huge ocean that is the World Wide Web. In a July 1999 report, computer scientists at the NEC Research Institute in Princeton calculated that there were some 800 million pages on the Web as of February 1999, more than double the 320 million pages they reported in December 1997.

Computer pedophiles (typically white, middle or upper class males, age 25 to 45) extol the virtues of sex with children and provide neophytes with child pornography. This psychological validation leads budding child molesters to believe that they are not strange or different after all and that it is society, with its laws declaring sex with children and child pornography to be criminal, that is wrong. They then continue the downward spiral into child exploitation, typically beginning by trading child pornography, progressing to sexually explicit online conversations with children, and eventually seeking child victims online for sex.

Computer pedophiles share methods and means by which to reduce a child's inhibitions and facilitate seduction. Ms. Aftab testified:

> What they're doing is teaching each other how to do it better so that when a child says, "It's okay to say no," because that's what we've told our children, they say, "When a child says to you, 'It's okay to say no,' this is your response," and they script out responses to get into the child's trust. … [Children] are not afraid of other children, not taught to be, so pedophiles come [online] pretending they're another child until they earn the trust of this child, and then they become a little bit older and a little bit older, and they meet them before they explain their true age or not.

Some authorities believe that the problem is too vast for Internet service providers to control, no matter how hard they might try to eliminate such sites. America Online, for example, has 20,000 chat rooms every night. So far, its own cyber-patrols — and even a computer system that monitors some rooms — have not prevented child pornography from being traded. Bounced from one room, computer-savvy pedophiles quickly create another and trade illicit images fearlessly. They have been known to hide their identities behind phony accounts financed with stolen credit cards or to use European e-mail systems

providing false identification numbers. Online, they trade information about encrypted programs and other ways to escape detection.

NO EASY SOLUTIONS

There are no simple solutions to resolve the twin problems of child pornography and molestation facilitated by computers. Rather, law enforcement agencies at all levels, school and library systems, private help organizations, software and Internet businesses, and concerned parents must join forces to decrease the risks to children. Legal solutions should be implemented, provided they do not curtail the immense capability of the Internet to communicate and inform for legitimate purposes.

Consideration is being given as to whether legislation should be proposed to amend *N.J.S.A.* 2C:7-1 to -6 to require that the information Megan's Law registrants provide (and update) in the registration form also should include all e-mail addresses the registrants use and any Web sites they own or operate. Such a measure would better enable the State Police to monitor the Internet activities of these individuals in order to ensure that they are not using the Web to disseminate child pornography, to lure minors, or for other illicit purposes.

The Internet neither knows territorial boundaries nor recognizes any nation's sovereignty. Effective law enforcement occurs only when officials shed turf consciousness and coordinate at all levels.

PARENTAL SUPERVISION

Most of the material on the Internet is not harmful to children. In fact, much of it is beneficial, fun and educational. No legal or technological panacea can prevent children from gaining access to corrupting material on the Internet without simultaneously depriving them of this enriching material. In the absence of foolproof screening measures, experts agree that parental supervision and an ongoing parent-child dialogue is key to having the Internet work for, not against, a child.

Parents should not allow young children to have unsupervised access to the Internet. They should instruct a child never to give out his or her full name, e-mail address, telephone number or home address to anyone met on the Internet. Friends in chat groups should receive similar instructions. Time on the Internet should be limited. Parents should explicitly tell their children never to arrange a face-to-face meeting with another computer user, even if it is another child, without parental permission.

Parents should encourage their children to report suggestive, obscene, or threatening e-mail or bulletin board messages. If a student uses a Web site to threaten violence toward his classmates, they may report it confidentially to the Executive Director of Cyber Angels, Parry Aftab, by clicking on KIDReportline at www.cyberangels.org.

It should be noted that the departments of Law and Public Safety and Education have taken a number of steps to protect children from hate crimes, which have the capacity to disrupt the educational environment, to inflame tensions, to cause emotional harm, and to presage outbursts of violence. The Attorney General's Education-Law Enforcement Working Group recently revised the "Uniform Statewide Memorandum of Agreement Between Education and Law Enforcement Officials" to deal specifically with hate crimes and bias-related acts committed by or against school-aged children. The Memorandum of Agreement, which all school districts are required to adopt and implement pursuant to regulations promulgated by the State Board of Education, spells out the procedures that school officials must follow in reporting hate crimes and bias-related acts (acts that are not criminal but that nonetheless are motivated by racial, gender, disability, religious, sexual orientation or ethnic prejudice and that have a potential to cause injury or provoke violent retaliation). The Memorandum of Agreement recognizes that a prompt, coordinated response is essential to defuse a potentially volatile situation and to prevent further physical or emotional injury. The text of the Memorandum of Agreement can be found on the Internet at www.state.nj.us/lps/dcj/index.htm.

The Customs Service's Gene Weinschenk testified:

> [S]tep one is to put the computer in your dining room, in your kitchen, in your den where people are going to go back and forth. If you walk back and forth a number of times and see a blank screen, the kids have a "hot button" set up. When they hear you coming, they hit the hot button, so you may want to take a look at what's going on.

Ruben Rodriguez, Director of the Exploited Child Unit, National Center for Missing and Exploited Children, testified about what a parent can do:

> … I keep telling [parents] the magic bullet basically is you, parental involvement, educating your children. The same things … you tell your children when [they] go out the door — "Cross on the green; don't talk to strangers" — all those things the parent does with the children, they forget those things when the child is home on the computer. …

> Unfortunately, we find that a lot of parents are computer phobic. They're still … thinking, "If I touch it, I'm going to blow up something." That's not true. I think it's better for the child to teach the parent on a lot of these issues so the parent can get involved, and just put some fundamental rules and regulations on the child so they understand what their problems are.

Parry Aftab authored *A Parents' Guide to the Internet … and how to protect your children in cyberspace* (SC Press 1997), a "user-friendly" book for parents interested in protecting their children from online pitfalls. Excerpts are available at www.cyberangels.org. Ms. Aftab has prepared a second Internet safety guide, *The Parent's Guide to Protecting Your Children in Cyberspace* (McGraw-Hill 2000), to replace her earlier book.

Ms. Aftab has drafted a contract for parents and children to sign and then post beside the family computer. It delineates a child's rights online, and may displace so-called "mommy hacking" — parents reading their children's e-mail and spying on their surfing activity — in households that have developed trust between parents and children. The contract is available at the Cyber Angels Web site. Children agree, among other things, to keep personal identifying information secret, to tell their parents about any pictures someone sends to them, to neither buy nor order anything without parental permission, and to seek parents' approval before calling or meeting anyone encountered online.

The federal Department of Education has a pamphlet entitled *Parents Guide to the Internet* (SC Press, Inc., November 1997). The booklet is available in English and Spanish on the Department's Web site at www.ed.gov/pubs/parents/internet.html. The guide gives parents an introduction to the Internet and suggests how they can allow their children to benefit from it while safeguarding them from its potential hazards.

The Children's Partnership has issued *The Parents' Guide to the Information Superhighway: Rules and Tools for Families Online* (2nd Ed. May 1998), available over the Internet at www.childrenspartnership.org. The guide was developed in conjunction with the National PTA and the National Urban League, with advisors including the American Library Association. *Child Safety on the Information Highway,* authored by Lawrence J. Magid, is available at www.safekids.com/child_safety.htm. It was produced jointly by the National Center for Missing and Exploited Children and the Internet Alliance (formerly the Interactive Services Association).

America Links Up: A Kids Online Teach-In, located at www.netparents.org, is a public awareness and education campaign sponsored by a broad coalition of non-profit organizations, education groups and corporations concerned with providing children with safe

and rewarding online experiences. Guides for online privacy are available from the Center for Media Education at www.cme.org.

BLOCKING, FILTERING AND MONITORING SOFTWARE AND CHILD-FRIENDLY BROWSERS

Abhorrent online material ranges from pornography to hate messages to information about the manufacture of bombs and psychotropic drugs. Software that denies access to such material can help parents protect their children from its inimical influence. It especially can help to protect younger children. Parry Aftab testified that such software is "relatively easy to install, and notwithstanding what a lot of people think, the kids really can't get around it. When you try, it will turn off and put up this big notice in red saying, 'Somebody tried to break into my system and go around it.'"

Censoring software has limitations, however, the most important being its tendency to lull parents into complacency. Their children's friends' houses, schools or public libraries may have computers that lack the software. Meanwhile, censorial software often screens out information that older children may find useful and non-offensive.

Blocking software prevents access to Web sites judged to be "bad" by the software maker. No matter how frequently the list of such sites is updated, however, the number of Web sites published each day far exceeds the ability of blocking software creators to review the sites and categorize them. Disturbing sites inevitably will get through.

Filtering software prevents access to sites containing certain keywords, alone or in context with other keywords. In addition to separate software, there are filtering features built into the popular Internet browsers (the software used to access the World Wide Web). Thus, parents can confine their children's access to those sites containing keywords that have been rated appropriate for children. The biggest problem with using keyword filtering, however, is that innocent sites may be blocked. In addition, some Web site operators have learned to circumvent the filtering by misspelling the keywords that typically are blocked.

Outgoing filtering software prevents children from sharing certain information, such as their names, addresses or telephone numbers. Even the best kids occasionally forget Internet safety rules. Indeed, sharing personal information online with strangers may be far more dangerous to children than seeing an image of a naked body or someone smoking a cigarette. Thus outgoing filters serve as an important safety valve.

Monitoring and tracking software allows parents to trace where their children go online, determine how much time they spend online,

and find out how much time they spend on the computer offline — playing games and the like. Some programs even permit parents to control what times of day their children can use the computer. This is particularly helpful when both parents are working outside the home, or when a working single parent is trying to control a latchkey kid's activities.

A directory of parental control resources may be found at www.safekids.com/filters.htm. It should be remembered, however, that engaged parents or guardians are the ultimate filter. Some screening, blocking or monitoring products are:

Net Nanny® (www.netnanny.com) from Net Nanny Software International, Inc.

Cyber Patrol® (www.cyberpatrol.com) from The Learning Company.

SurfWatch™ (www.surfwatch.com) from JSB Software Technologies.

CYBERsitter™ (www.cybersitter.com) from Solid Oak Software, Inc.

Cyber Snoop™ (www.pearlsw.com) from Pearl Software, Inc. is an "after the fact" analysis tool that allows parents to view a record of their child's Internet activity. A click of the "history" tab, or its equivalent, on a browser tool bar will produce a list of links to every site the computer has visited recently. Although computer-savvy youths know how to delete incriminating evidence, programs such as Cyber Snoop create a tamperproof database.

Bess® (www.n2h2.com) is an Internet filtering service from N2H2®, Inc. The firm also markets Searchopolis, a filtered search engine and resource site for K-12 students.

Internet Manager™(www.elronsoftware.com) from ELRON Software, Inc. tracks, reports, and, if necessary, blocks inappropriate Web surfing.

FoolProof Internet™ (www.smartstuff.com) from SmartStuff Software provides content filtering, guided activities and browser control.

Disk Tracy™98 (www.disktracy.com) is a product of WatchSoft, Inc.

One Tough ComputerCOP (www.bestalert.com/beaudietl/computer.htm) was developed by a former NYPD detective. It permits parents to determine if their computers are being used to access offensive material. It also retrieves deleted files if they have not been overwritten.

The Disney/Infoseek GO Network™ (www.go.com) offers the regular staples of a Web portal: search engine, free e-mail, yellow pages, maps and news. It also has GOguardian™, a way to filter out "adult" content, such as pornography, in Web searches.

Preference options are available in both leading Web browsers: Netscape Navigator and Microsoft's Internet Explorer. Child-friendly browsers, such as KidDesk Internet Safe from Edmark Educational Software, Surf Monkey from MediaLive, and Bandai Interactive, limit access to all but pre-selected sites.

The AltaVista™ search engine offers AV Family Filter at http://doc.altavista.com/help/search/family_help.shtml. It filters objectionable content in partnership with SurfWatch™. It blocks sites pertaining to drugs, alcohol, tobacco, gambling, hate-filled speech, explicit sex, and violence. Lastly, it removes inappropriate pages reviewed by editors and AltaVista users.

Bright Mail (www.brightmail.com) from Brightmail, Inc. is a free service that screens out unwanted "spam" — unsolicited e-mail. It routes a consumer's e-mail through the company's computers, scans for telltale signs of spam and forwards everything else to the consumer's electronic mailbox. It filters out bulk messages with sexual or get-rich-quick themes and blocks messages from known spammers. The consumer receives a message each week listing the spam messages found. The service does not yet work with certain ISPs, most notably America Online.

America Online, the ISP used by more than 22 million households, allows parents to limit incoming e-mail to a finite list of "approved" correspondents. AOL also has built-in settings that can bar children from all but full-time-monitored chat rooms and pre-screened kid-friendly Web sites.

CHILD-FRIENDLY WEB SITES

New Jersey Hangout: www.state.nj.us/hangout. The site contains Internet safety tips and links to child-friendly Web sites.

Kids Page: www.usdoj.gov/kidspage. The U.S. Department of Justice has provided information to guide children of different age groups safely through the Internet.

Yahooligans: www.yahooligans.com.

Mamamedia: www.mamamedia.com.

Kid's Wave: www.safesurf.com/kidswave.htm. This site features a partial list, organized by age-appropriateness, of Web sites that have received the SafeSurf™ seal of approval.

Ask Jeeves for Kids: www.ajkids.com.

KidsClick! provides a Web search for kids by librarians at http://sunsite.berkeley.edu/KidsClick!.

American Library Association's Great Sites for Kids: www.ala.org/parentspage/greatsites/amazing.html. This site lists 700-plus Web sites compiled by the Children and Technology Committee of the Association for Library Service to Children, a division of the American Library Association.

The Boston Computer Museum maintains a list of sites for children and teens, including various e-zines, at www.tcm.org/html/info/education/programs/interact/kids-list.html.

Web Wise Kids™: www.webwisekids.org.

Child Lures: www.childlures.com.

SCHOOL AND LIBRARY POLICIES

A minimal number of students actively seek inappropriate material at school. According to Arthur Wolinsky of Barnegat, a consultant for Southern Regional High School District in Manahawkin and an expert in online safety for school children, schools had more problems with inappropriate use of the Internet back in 1995 when computers were in schools but not yet abundant in homes. Students now can access forbidden sites in their own homes, or in the homes of their friends. Therefore, they rely on school computers less for that purpose.

When an incident does take place in a school, inadequate supervision usually accounts for it. School districts must provide proper training to their teachers and administrators so that they may ensure a safe, quality online environment in the classroom. Organizations such as the non-profit Online Internet Institute (http://oii.org/index.html), where Mr. Wolinsky is the Technical Director, help educators to safely and effectively involve cyberspace resources in the learning process.

Just as it is not a panacea against the intrusion of objectionable material into home computers, screening software is not the ultimate solution for preventing such material from invading school computer networks. Schools also need to adopt and fully implement effective acceptable use policies (AUPs) for filtered and unfiltered stations on their networks.

The New Jersey Department of Education (DOE) has been providing information to school districts to help them protect students from dangers posed by inappropriate use of interactive technology systems such as the Internet. The state's High Technology Crimes and Interactive Computer Services Protection Act, effective May 1, 1999, requires the DOE to recommend guidelines and curriculum materials to local school districts on the ethical use of computers and the potential dangers to juveniles posed by those who use interactive computer services for illegal purposes. The law mandates that school districts include such information in their computer instruction, as well as safe computing guidelines made available by the Department of Law and Public Safety. DOE's Web site to accomplish these tasks is www.state.nj.us/njded/techno/htcrime/index.html.

DOE's Web site links to the text of the new law, sources of filtering software and examples of AUPs developed by various school districts. It contains current information on the debate between those who would rely primarily on filtering programs and those who would make students responsible for appropriate use of interactive technology through clear AUPs. DOE has not adopted or imposed a model acceptable use policy on local districts. An effective information access policy (IAP) would probably involve some filtering, at least in the lower grades; some instruction about dangers and ethics; and some way to use unfiltered stations safely. Teachers need proper professional development in this area. Schools need monitoring software to track sites that students access and to check e-mail generated by or coming into school computers.

The situation is complicated by free Web-based e-mail accounts offered by hundreds of providers. They are anonymous and easy to access. Also, Web-based chat rooms and communities have proliferated. It has been suggested that New Jersey's 21 Educational Technology Training Centers (ETTCs) could provide a controlled e-mail, chat and conference environment for students and teachers in schools that cannot afford their own servers.

Meanwhile, there are many child-safe educational chat events in which students may participate with their teachers. Making teachers aware of these services offers them alternatives to the open chat areas that present problems. Cable in the Classroom, located at www.ciconline.org, operates the Professional Development Institute, which is the centerpiece of a new cable-TV industry program to provide free Internet training and educational resources to teachers in 1999 and 2000. The site helps educators to overcome the technology gap.

The New Jersey School Boards Association hosted a July 1998 conference for school board leaders on "Perils of the Internet." It also held a curriculum conference on March 20, 1999 entitled "The

Internet – Policy and Perils." The Association's Web site, www.njsba.org, provides some links to Internet safety information.

Project Fairfax, in the Virginia town of that name, recognizes that child sexual predators, particularly those utilizing the Internet, cannot be stopped by law enforcement activity alone. Prevention and community involvement also must attack the problem. Thus the CyberSmuggling Center, the Fairfax County Police Department, the Fairfax County Public School System, the Fairfax County Library System, the Fairfax County Social Service Agency, and the National Center for Missing and Exploited Children have all joined in a coordinated assault on the problem. In March 1999, the Fairfax County Public School System contracted with URLabs for its I-Gear software (www.urlabs.com) to manage classroom Internet access.

In New Jersey, the Somerset Hills School District is testing CyberSmart!, a non-profit program developed by Bernardsville resident James Teicher. The program instructs teachers to give students tips on how to avoid online sexual predators. WebManager (www.sagebrushcorp.com) from Sagebrush Corp. provides Internet content management for schools and libraries.

Parry Aftab reported that Cyber Angels has worked with the Baltimore County School System in Maryland to set up Parents Internet Education, the largest program of its kind in the country. Her book, *A Parents' Guide to the Internet,* also is provided to schools on a courtesy basis. In addition, a security company in Seattle produced a video that dramatically illustrates dangers children may encounter on the Internet. The video is distributed free to schools. Meanwhile, volunteers on the Cyber Angels Sites Team rate Internet sites on their suitability for children.

In April 1999, Ms. Aftab started a program called Teen Angels. Local law enforcement, the FBI and Ms. Aftab trained volunteer high school students. In early October 1999, they began instructing Ridgewood School District students how to teach online safety to their peers.

As is the case with schools, libraries must serve as guardians of Internet safety. This includes the implementation of effective policies to ensure safe and lawful online activities. The American Library Association created *The Librarian's Guide to Cyberspace for Parents & Kids,* www.ala.org/parentspage/greatsites/guide.html, a Web site providing safety tips, help for parents and a list of "great sites" for children and parents. Some libraries set aside filtered Internet access stations for children. Others issue electronically coded cards to Internet users. The cards permit different levels of access according to age and parental consent. People over 18 can choose any level they want.

Nancy Willard is an Oregon-based educator, lawyer and information technology consultant. She wrote *A Legal and Educational Analysis of K-12 Internet Acceptable Use Policies*, www.erehwon.com/k12aup/legal_analysis.html.

The Children's Internet Protection Act (S.97), sponsored by U.S. Senator John McCain (R-AZ), would pressure schools and libraries to filter sexual material received from the Internet. Those that did not comply would be denied a portion of a recently created $1.9 billion-a-year fund (paid by telecommunications companies and collected by the Federal Communications Commission) available to pay for new Internet service. The bill would leave it up to the local school district and library board to determine the type of filtering technology to use. A related bill is H.R. 543, whose primary sponsor is Robert Franks (R-NJ), Co-chair of the Congressional Missing and Exploited Children's Caucus. Critics of the bills include the National Education Association, the American Library Association, and the Internet Free Expression Alliance (an ad hoc group whose members include the ACLU, the American Society of Newspaper Editors and People for the American Way). The critics say the technology is far from foolproof and contend that control decisions should be made locally and with great respect for the First Amendment.

CONTROL ORGANIZATIONS AND PROGRAMS

The United States has begun the process of assembling a combined force of computer crime law enforcers, at federal, state and local levels, aided by official prevention programs and private organizations and individuals that report offenders and educate the public. There should be a national clearinghouse to keep track of all of the investigations. Otherwise, as more law enforcement agencies begin to conduct isolated investigations, incidents of one agency investigating another's undercover operation will become more common. This obviously would waste very limited resources.

If a member of the public comes across child pornography on the Internet, he or she should not download the material and forward it to an enforcement agency. This is a violation of law. If it were not unlawful, child pornographers could cite their desire to complain about images as the reason for having them in their systems. Therefore, instead of downloading an offending image for forwarding, the site name should be noted and passed on to law enforcement.

UNESCO

Since computer systems do not respect even international boundaries, a worldwide effort must be made to control online child exploitation. An eight-member UNESCO (United Nations Educational, Scientific and Cultural Organization) committee is preparing worldwide

plans for online safety and activity to counter child pornography and pedophilia over the Internet. The committee arose out of a January 1999 U.N.-sponsored conference in Paris on child exploitation and the Internet. Parry Aftab is the only American on the committee, which will implement an initiative: World Citizens Movement to Protect Innocence in Danger. Ms. Aftab is presiding over and forming the U.S. National Action Committee, which will serve as a model for the national action committees of Internet-developed nations.

The Innocence in Danger program will help to set up "electronic watchtowers," international cyber-hotlines serving different populations. One hotline will help child abuse victims obtain help from parents, police, peer counselors and medical professionals. Another "umbrella" tip line will permit anyone, anywhere in the world, to report a violation and direct the complainant to the proper jurisdiction. A network of volunteers will monitor the tip line. It also will link the international law enforcement community, allowing users to share information and expertise online. Worldwide child Internet safety programs will involve schools, libraries and community groups. Programs will educate parents about the Internet. More information may be obtained at www.familyguidebook.com.

An organization chart showing the U.S. National Action Committee and its industry task force advisory committees is at www.cyberangels.org/unescochart1.html. The relevant UNESCO Web site may be found at www.unesco.org/webworld/child_screen/index.html.

Often, there are no international treaties to allow extradition of violators. Another problem is the disparity in laws from country to country. Fewer than a dozen of the world's nearly 200 countries have laws that specifically address child pornography. A computer operator in the United States who downloads illegal images is guilty of a federal crime and can be prosecuted, but U.S. laws cannot be applied to overseas child pornography dealers. At UNESCO's annual meeting in June 1999, members supported measures that would ban online child exploitation, including the sale and trafficking of child pornography over the Internet.

WHITE HOUSE

In June 1998, the White House held a Summit on Online Content for Children. At an earlier, three-day Internet Online Summit for Kids in December 1997, a "zero tolerance" policy on Internet child pornography was announced. It called for increased cooperation between leading Internet service providers (ISPs) and law enforcement. Most participants indicated they would prefer to rely largely on market solutions, such as software that filters out risqué material and systems allowing Web sites to rate themselves.

The initiative included the National Center for Missing and Exploited Children's CyberTip Line. It also created a national public-awareness campaign called "Think Then Link" to educate parents about the benefits and dangers of the Internet. In addition, it included a free Education Department manual, *Parent's Guide to the Internet*, written to help parents find educational sites online. The entire book is available on the DOE's Web site at www.ed.gov/pubs/parents/internet.html. Lastly, key ISPs agreed to remove child pornography from their own bulletin boards and services.

FEDERAL BUREAU OF INVESTIGATION AND OFFICE OF THE U.S. ATTORNEY FOR THE DISTRICT OF NEW JERSEY

The FBI's William Megary testified about the Northeast Regional Child Exploitation Task Force (NERCET), which has been at work since December 1998. Authorities decided to publicize the existence of the Task Force as a deterrent. The Task Force, which may be reached at 732-469-7986, focuses on those suspected of using the Internet to meet children for sex or to produce, manufacture, distribute or collect child pornography. Usually, either the victims or perpetrators in Task Force cases are located in New Jersey.

The Task Force is based on the Baltimore FBI Office's "Innocent Images" undercover operation, which began in 1995. The Task Force has six investigators — three from the FBI and one each from county prosecutors' offices in Bergen, Somerset and Middlesex counties. The FBI also has assigned research specialists to the Task Force. The investigators pose as children in cyberspace in order to catch sexual predators. Mr. Megary indicated that a half dozen counties were asked to join the Task Force, but only three decided they could dedicate limited personnel on a full-time basis.

Since 1995, Innocent Images has produced hundreds of convictions for sex crimes facilitated by the Internet. New Jersey's NERCET had made 34 arrests as of March 2000. Two children were recovered from "travelers" coming from their home states to have sex with children they met online. A similar task force will exist in every state before the year 2000 ends.

The FBI has required that all of its online child pornography and child sexual exploitation investigations be coordinated by Innocent Images' central operation at the Maryland Metropolitan Office, Baltimore Division. This may serve as an example for a much-needed national clearinghouse of online child exploitation investigations by all interested agencies and organizations.

As part of the Innocent Images program, the FBI conducts training seminars around the country aimed at helping local police departments upgrade their computer skills. One such seminar, held in Morris Township, New Jersey, in mid-1998, stressed the importance of Internet

knowledge as a vital investigative technique to outwit computer-savvy child predators.

A successful example of a task force with FBI support is the Sexual Assault Felony Enforcement (SAFE) Team. A regional law-enforcement group, SAFE is made up of officers from local, state and federal agencies in California. Since its inception in 1995, SAFE has investigated various types of child exploitation cases, including pornography, molestation and abductions. The team covers seven counties. A FBI supervisory agent manages the program. An assistant United States Attorney prosecutes cases investigated by SAFE.

In New Jersey, an assistant United States Attorney devotes full time to prosecuting child endangerment cases. She has handled these matters for 18 years and works with county prosecutors' offices to divide up the cases. She now gets three or four calls for assistance per week from state authorities.

In 1998, the FBI published *A Parent's Guide to Internet Safety*. Free copies are available from the FBI's Office of Crimes Against Children, 935 Pennsylvania Avenue N.W., Washington, D.C. 20535, (202) 324-3666, or from its New Jersey Division Office, 22nd Floor, Gateway 1, Market Street, Newark, New Jersey 07102 (973) 622-5613. It also may be viewed on the FBI's Web site at www.fbi.gov.

The FBI's National Sex Offender Registry – a computerized database of convicted pedophiles – became operational in mid-summer 1999. It makes background checks immediately available to law enforcement agencies. State participation in the registry, however, is voluntary.

UNITED STATES CUSTOMS SERVICE

The United States Customs Service's Child Pornography Enforcement Program was established in 1985. Its CyberSmuggling Center was created in August 1997. The Center focuses primarily on child pornography and child sexual exploitation. It averages one child pornography-related arrest every two days.

The CyberSmuggling Center also trains and assists state, local and foreign law enforcement. The Center's telephone Tipline is 1-800-BE-ALERT, and its Web site is www.customs.treas.gov (click on "Enforcement" and then "Reporting Child Pornography"). In a joint project with the Florida Department of Justice, the Customs Service has collected online resources for parents and children who want to learn more about general Internet safety and how to recognize and avoid child predators. Its Web site is www.fdle.state.fl.us/publications/safety_forum/index.html.

FEDERAL TRADE COMMISSION

A 1998 Federal Trade Commission (FTC) survey of 212 child-oriented Web sites found that 89 percent of them collected personal information, but only one percent required parental consent. In October 1999, the FTC issued a trade regulation to implement the Children's Online Privacy Protection Act, which was enacted in late 1998. The law and regulation, which the FTC began to enforce on April 21, 2000, control the collection over the Internet of personal identifying information about children. The aim is to keep such information out of the hands of people who might use it to harm or exploit children.

The new law requires commercial Web sites generally to obtain "verifiable parental consent" before asking children under 13 for their names, addresses, telephone numbers or other identifying information. Under the new FTC regulation, Web sites that share children's information with other companies must obtain a parent's permission through mailed or faxed paperwork, telephone calls to a toll-free number, use of a credit-card number, or e-mail using a password or budding "digital signature" technology. In two years, the FTC will consider whether e-mail can be more widely used to seek a parent's permission, as techniques improve for ensuring the identity of e-mail authors.

NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

The National Center for Missing and Exploited Children (NCMEC) (www.ncmec.org) based in Arlington, Virginia, is a private, non-profit organization established in 1984. Operating under Congressional mandate, it works with the United States Department of Justice's Office of Juvenile Justice and Delinquency Prevention. It trains police and other professionals. Its toll-free CyberTipline (1-800-THE-LOST) is run by a grant from the DOJ. The Center operates the CyberTipline, online since March 1998 at www.missingkids.com/cybertip (www.cybertipline.com), in conjunction with the U.S. Customs Service, the U.S. Postal Inspection Service and the FBI. The Center is working with Internet service providers to promote the Tipline to their members. Some have, and some have not.

On April 23, 1998, more than 50 law enforcement officers and social workers from throughout central New Jersey took part in a live national conference, "Protecting Children Online," via remote video hookups. Somerset Medical Center in Somerville donated its satellite-ready auditorium for the forum, sponsored by NCMEC and the Department of Justice, which has a Child Exploitation and Obscenity Section. Detective Mark Butler of the Somerville Police Department organized the conference, in which the FBI also participated.

NCMEC offers two free brochures: *Child Safety on the Information Highway* and *Teen Safety on the Information Highway*. They may be obtained by writing to NCMEC at 2101 Wilson Blvd., Dept. P, Suite 550, Arlington, VA 22201-3077.

OFFICE OF JUVENILE JUSTICE AND DELINQUENCY PREVENTION

In 1984, Congress enacted the Missing Children's Assistance Act, which established the Missing and Exploited Children Program (MECP) within the Office of Juvenile Justice and Delinquency Prevention (OJJDP). The MECP provides services to children, parents, educators, prosecutors, law enforcement, and other professionals and interested persons working on child safety issues. OJJDP brought its MECP Web site online in April 1998. The Web site (http://ojjdp.ncjrs.org/missing) provides children with information to help them avoid cyber-exploitation.

In 1998, OJJDP (www.ojjdp.ncjrs.org) created the Internet Crimes Against Children (ICAC) Program to respond to the emerging threat of sex offenders using computer-facilitated online technology to sexually exploit children. The initiative develops training and technical assistance programs to assist state and local law enforcement agencies in responding more effectively to the threat and to stimulate creation of regional multidisciplinary task forces. At the end of 1999, law enforcement agencies in 10 different states, not including New Jersey, received assistance awards to implement regional task forces to address and combat Internet crimes against children. This brought the total number of states with ICAC programs to 20. The task forces include representatives from law enforcement, victim services, child protective service agencies, and other relevant government and non-government agencies. According to the U.S. Department of Justice, since the monetary awards were given to the initial 10 states, more than 100 individuals have been arrested for sexually exploiting children over the Internet.

Under the ICAC Program, federal funds are used to implement safety education and prevention programs for children, parents and educators; to develop response protocols that foster collaboration, information sharing and service coordination; and to acquire sophisticated training and cutting-edge equipment for investigators. Ideally, the task forces will become part of a national law enforcement network that will assist parents, educators, prosecutors and other professionals working on child protection issues. In 1999, OJJDP awarded funding to a minimum of eight additional jurisdictions to develop and support regional law-enforcement task forces to address the problem of Internet crimes against children.

OJJDP and NCMEC, in consultation with the FBI, U.S. Customs Service, U.S. Postal Inspection Service and the Child Exploitation and Obscenity Section of the U.S. Department of Justice, developed new law

enforcement training programs and sponsored a national teleconference. The teleconference provided information regarding prevention, investigation, applicable federal law and available resources to more than 30,000 viewers in over 400 down link sites. The training courses, Protecting Children Online and Protecting Children Online Unit Commander, were developed for law enforcement investigators and managers. In 1998, more than 400 law enforcement executives and investigators participated in the two courses.

In 1999, OJJDP selected from competitive proposals to develop an ICAC Task Force Training and Technical Assistance Program. The Program will deliver advanced technical training related to computer-facilitated sexual exploitation offenses, convene ICAC town meetings, support the ICAC Task Force Review Board and assist task force development in other ways determined by OJJDP.

CYBER ANGELS AND OTHER HELP ORGANIZATIONS

Cyber Angels (www.cyberangels.org) has operated since June 1995 as the largest online safety and educational program in cyberspace. Parry Aftab has served as its Executive Director since mid-1998. Her Web site is located at www.familyguidebook.com. Cyber Angels has hundreds of volunteers worldwide, including “hunt-and-track” specialists, who submit to background checks. These volunteers use special software and training to locate child pornography and suspected predators online. They report leads to law enforcement agencies.

Dr. Nancy Faulkner is the Executive Director and Debbie Mahoney is the Founder and President of Safeguarding Our Children — United Mothers (SOC-UM). Its Web site is www.soc-um.org. SOC-UM manages Cyber Angels’ Internet Patrol. Dr. Faulkner also produces Pandora’s Box: The Secrecy of Child Sexual Abuse, located at www.prevent-abuse-now.com.

Safe Kids International, www.skig.org, operated by Joseph Florentine and Gary Schrader in Spring Lake, New Jersey, uses the Internet to locate missing, runaway or abducted children. Akin to using online milk cartons, the company sends pictures and information about missing children to a network of volunteer “points of contact” on the Internet.

The Internet Education Foundation runs GetNetWise, www.getnetwise.org, which is sponsored by a consortium of non-profit organizations and major corporations to help parents keep their children safe in cyberspace. With the help of the American Library Association and others, GetNetWise serves as a global clearinghouse of tools to assist parents to screen out and report objectionable material, monitor the amount of time their children spend online, and tell where the children have been on the Internet. The site has a glossary of Internet terms, a guide to online safety, directions for

reporting online trouble, a directory of online safety tools, and a list of sites suitable for children to visit.

Lawrence Magid, a child online safety advocate, heads the Online Safety Project and created SafeKids.Com (www.safekids.com) and SafeTeens.Com (www.safeteens.com). He also wrote *The Little PC Book* (Peachpit Press) and the brochures *Child Safety on the Information Highway* and *Teen Safety on the Information Highway*, both produced by the National Center for Missing and Exploited Children.

Another helpful site is www.klaaskids.org, which is run by the Klaas Foundation for Children of Sausalito, California. Captive Daughters is a Los Angeles-based group that works against sexual trafficking. It may be reached at 1-888-300-4918 or www.captive.org. PedoWatch is a non-profit organization monitoring pedophilia on the Internet. Its Web site is www.pedowatch.org. Enough Is Enough actively campaigns against pornography and online predators at www.enough.org. AntiChildPorn Org (ACPO), founded in March 1999, has over 500 members that go after child pornography sites by providing detailed information to law enforcement officials. Its Web site is www.antichildporn.org. The Child Welfare League of America (CWLA), www.cwla.org, developed a ten-year national campaign, called "Protecting America's Children: It's Everybody's Business,®" to stop child abuse and neglect and to promote child protection as a community-wide responsibility.

Members of some anti-child pornography organizations may cross the line into illegal vigilantism during well-intentioned efforts to shut down offending sites. It has been reported that some people affiliated with Hackers Against Child Pornography, Ethical Hackers Against Pedophilia (www.ehap.org) and Condemned.org (www.condemned.org) have resorted to hacking into Web sites to take them offline. When efforts to work with Internet service providers and law enforcement have failed to elicit responses deemed sufficiently rapid, such activity may occur, even though it may violate the posted policies of some of the organizations.

Erasing hard drives and getting rid of information destroys evidence that law enforcement could use to prove a case in court. Information gathered by illegal means and turned over to police and prosecutors may later prove inadmissible in court. Moreover, shutting down a site is only a minor inconvenience to the person possessing and posting child pornography. Unless brought within the justice system, the predator is still able to continue harming and exploiting children. Meanwhile, anti-porn hackers may themselves be committing crimes by removing material that no court has yet ruled to be obscene.

END CHILD PROSTITUTION AND TRAFFICKING (ECPAT) AND THE WORLD TOURISM ORGANIZATION (WTO)

End Child Prostitution and Trafficking (ECPAT) is a global network of organizations and individuals campaigning in over 30 industrialized and developing nations against child-sex tourism, child prostitution and child pornography. Such activities often are advertised on the Internet. ECPAT-USA, based in New York City, (212) 870-2427, tries to convince travel businesses to distribute a brochure it produced on sex tourism, entitled "What You Should Know About Sex Tourism Before You Go Abroad." The brochure points out that under the federal Child Sex Abuse Prevention Act of 1995, Americans can be prosecuted for traveling overseas to have sex with minors. Along with INTERPOL, ECPAT in 1997 published a 24-page booklet entitled "Child Pornography on the Internet."

In 1998, the World Tourism Organization (WTO), www.world-tourism.org, the 133-member United Nations tourism body, launched an international campaign against child-sex tourism. Based in Madrid, Spain, the WTO adopted a "No Child Sex Tourism" logo to be emblazoned on airline-ticket jackets, ads and hotel door tags. The WTO has urged the prosecution of companies, individuals, agencies and clubs involved in the promotion of child sex tourism and the punishment of tourists involved in the sexual exploitation of children.

INTERNET SERVICE PROVIDERS

Certain Internet service providers (ISPs) cooperate with law enforcement, but they will identify clients only when served with search warrants or subpoenas. That makes investigations difficult, because e-mail records are kept for only a few days. ISPs keep membership records at best for only a few months after a customer leaves. E-mail messages that have been read are stored for just a couple of days, or not at all. Some providers do not keep any records.

According to D. Douglas Rehman, President of Rehman Technology Services, Inc., a computer security firm, child pornography is principally confined to a few known newsgroups (sometimes called bulletin boards). Internet service providers (ISPs) subscribe to thousands of newsgroups. When someone makes a posting to a specific newsgroup, it is sent across the Internet. Any ISP that subscribes to that newsgroup will receive that posting and maintain it on its system for a set number of days or weeks. ISPs could discontinue carrying exploitative groups or they could utilize software that would strip images from postings but allow text postings in those newsgroups.

Some ISPs have programs to counter child pornography and exploitation. America Online prepared a training video for law enforcement. It also regularly turns over customer complaints to authorities. Safe Surfin', located at www.safesurfin.com, is a safety

site from AOL that includes an Internet Driver's Ed quiz, tips from teen actors and other celebrities, and useful links.

NEW JERSEY STATE POLICE

The High Technology Crime and Investigations Support Unit (HTC&ISU) in the Division of State Police investigates traditional crimes that involve the use of computers, such as forgery, fraud, theft by deception, terroristic threats, narcotics distribution and organized crime activities. It also investigates crimes that have developed with advances in technology, such as "cyberstalking." The Unit also patrols the Internet daily looking for adults seeking sexual encounters with minors. In addition to its own patrols and investigations, the HTC&ISU assists other states with criminal investigations. Recent cooperative operations included efforts to prevent the luring of children over state lines, securing search warrants and arresting suspects. The Unit also has assisted out-of-state authorities with curtailing the manufacture and distribution of child pornography.

LAWS AND LEGAL ACTIONS

Lawmakers recently have hardened New Jersey's stance against child pornographers, both within and outside of cyberspace.

New Jersey's Computer Pornography and Child Exploitation Prevention Act of 1998, *P.L.* 1998, *c.* 126, was signed by the Governor on October 22, 1998 and took effect on April 1, 1999. Assemblywoman Rose Marie Heck sponsored the legislation and chaired a committee that held hearings on the subject in late 1997. It is now a crime of the second degree to communicate child pornography to a child — any person under 16 — via a computer or to lure or entice a child into sexual acts. The conduct is a first-degree crime if done by a parent or guardian. The law also clarifies that the crime of endangering the welfare of a child includes use of the Internet for child pornography or enticement. Moreover, the commission of these crimes, or contacting a child unlawfully via the Internet, provides grounds for a civil action. Strict liability applies if the child is under 16.

New Jersey obscenity law amendments, *P.L.* 1999, *c.* 227, were signed by the Governor on September 30, 1999 and took effect on November 1, 1999. Under the amendments, a person showing obscene material to a person under the age of 18 is guilty of a crime of the third degree if the perpetrator is at least four years older than his victim and the showing is done with the knowledge or purpose to arouse, gratify or stimulate the offender or another. Since "show" is defined as "cause or allow to be seen," it probably includes the act of transmitting for display on a computer screen.

Federal laws dealing with sex crimes against children are tougher than state laws, and federal authorities can pursue a case across state lines more easily than state officials can. Moreover, federal law puts the age of consent for sexual activity at 18, whereas New Jersey's age of consent is 16.

Under the Child Protection Act of 1984, the U.S. Customs Service received the authority to investigate any cases involving the receipt, transmission, manufacture or possession of child pornography shipped in foreign commerce. In 1988, Congress passed a law outlawing the use of a computer to transmit, manufacture or possess child pornography shipped in foreign commerce.

In June 1997, the U.S. Supreme Court struck down portions of the federal Communications Decency Act of 1996 on First Amendment grounds, *Reno v. American Civil Liberties Union*, 117 *S.Ct*. 2329 (1997). The law applied to non-commercial as well as commercial Web sites. The court struck down Congress' effort to protect children from sexually explicit, but not legally obscene, material. However, on April 19, 1999, the Supreme Court, on direct appeal from a three-judge trial court, unanimously affirmed the law's ban on obscene e-mail. Such material must be more than merely indecent. The free-speech protection is lost only if the material appeals to prurient interests and depicts sexual conduct in a patently offensive way. The determination is left to a jury applying contemporary community standards.

The federal Child Online Protection Act (COPA) was signed into law on October 21, 1998. It requires commercial Web sites to collect credit card numbers or other access codes as proof of age before allowing Internet users to view material deemed "harmful" to children under 17. Violators are subject to up to six months in jail and a fine of up to $50,000 per day. In November 1998, the federal District Court for the Eastern District of Pennsylvania temporarily restrained the government from enforcing the law. *American Civil Liberties Union v. Reno,* No. 98-CV-5591 (E.D. Pa.). The court issued a preliminary injunction on February 1, 1999, shielding Web site operators from prosecution.

The Child Protection and Sexual Predator Punishment Act was signed into law on October 30, 1998, after Congress heard unspeakable accounts of sexual predators making initial contact with their child victims via the Internet. An amendment inserted by Representative Robert D. Franks (R-NJ) requires Internet service providers to report incidents of suspected child pornography to authorities or face fines of up to $10,000. The new law:

- Prohibits contacting minors (those under 18 years old) on the Internet, or through e-mail, for the purpose of engaging in any sexual activity or transferring "obscene matter."

- Increases penalties for a variety of sex crimes, including doubling the maximum prison term from five to 10 years for enticing a minor to travel across state lines to engage in illegal sexual activity and imposing a 15-year maximum term for persuading a minor to engage in prostitution or a sexual act.
- Authorizes pretrial detention of federal sex offenders.
- Prohibits unsupervised access to the Internet by federal inmates and encourages state officials to impose a similar ban on state inmates.
- Provides for a prison term of up to five years for using the Internet to transmit the name, address, telephone number or other information about a minor for the purpose of encouraging or soliciting criminal sexual activity.

The federal Child Pornography Protection Act of 1996 was adopted to combat the use of computer technology to produce pornography that conveys the impression that children were used in photographs or images. The technology enables someone to take a perfectly innocent picture of a child and alter it to show the child engaged in sex. The simulation can be used by a pedophile to entice a child. In April 1998, the federal District Court in Maine ruled that the part of the law that defines child pornography as a visual depiction that "appears" to be a minor engaging in sex was unconstitutionally vague. Meanwhile, a federal District Court in California ruled that the law was constitutional.

In 1997, FBI Director Louis J. Freeh told Congress that, although the transmission of child pornography over the Internet is illegal, many potential cases are neither pursued nor prosecuted because federal guidelines generally require that a suspect be shown to have committed the offense at least three times.

New Jersey officials may charge a fourth degree crime against those who “publicly communicate” over the Internet obscene material to a person under age 18. *N.J.S.A.* 2C:34-4. In 1998, the statute establishing the crime of endangering the welfare of a child was clarified to include offenses involving child pornography on the Internet. Any person who knowingly disseminates child pornography via the Internet is guilty of a crime of the second degree in New Jersey. *N.J.S.A.* 2C:24-4b(4)(a). Knowingly possessing or viewing child pornography obtained via the Internet constitutes a crime of the fourth degree. *N.J.S.A.* 2C:24-4b(4)(b). If the child depicted in a prohibited sexual act or simulation is under the age of 16, the responsible party is held strictly liable. *N.J.S.A.* 2C:24-4b(5).

BIAS AND HATE

THE PROBLEM

All of society degenerates when individuals or groups infringe the rights of others through prejudice against race, religion, gender, ethnicity, sexual orientation, disability or occupation. Cyberspace permits hate mongers, bigots, racists waging what they call “RAHOWA” (RAcial HOly WAr), extremists, Holocaust deniers, militias, "common law courts," anti-government radicals, anti-Semites and immigrant bashers to reach vast new audiences of potential adherents. Hate groups taking advantage of the new technology include the Ku Klux Klan, neo-Nazis, skinheads, Christian Identity, black separatists and a host of others.

The membership of hate groups includes individuals from all walks of life, who often trade business suits for Klan hoods, swastikas and other emblems of hatred and intolerance. They exploit anti-government sentiment, fears about non-white immigration, and demeaning theories of so-called “race scientists” to expand extremist movements with racist underpinnings.

According to the Intelligence Project of the Southern Poverty Law Center (SPLC), 457 hate groups operated in the United States in 1999, including five in New Jersey. To be included in this count, the groups had to engage in racist behavior involving crimes, marching, leafleting or publishing literature. Noting a 15 percent drop in the number of such groups from the previous year, the SPLC pointed out in a March 2000 report that “many individual white supremacists have retreated to the Internet — increasing their propaganda reach but diminishing the numbers of people actively engaged in the movement in other ways.” The report continued:

> The number of such individuals is growing. In 1998, 95 of the 254 [U.S.-based] hate Web sites were not affiliated with hate groups active beyond cyberspace — 37% of the total. In 1999, the number of unaffiliated sites swelled by 50% to 143 — 47% of the 305 hate sites that the Intelligence Project counted in early 2000.

The SPLC report added that several of the largest hate groups have increased in size as they absorbed members of smaller groups. Thus, the reduction in the number of small groups has been offset by the increase in membership in large groups.

White supremacist and neo-Nazi Web sites support hate groups financially through e-commerce sales of hate rock recordings and other paraphernalia. Much of the activity is underground. For example, hate

rock concerts, their locations rarely announced far in advance, are promoted, in part, by e-mail limited to sympathizers and potential sympathizers.

According to the SPLC, 523 so-called "patriot" organizations operated in America in 1998. In New Jersey, they include the U.S. Taxpayers Party based in Cinnaminson, the New Jersey Militia based in Trenton, with at least one offshoot in Salem County, the Council of Conservative Citizens and the New Jersey Committee of Safety based in Shamong. At least five of the top hate rock bands, showcased on such hate Web sites as Pillage and Plunder and Hammerskin Nation, are based in New Jersey. The five are Dying Breed; Aggravated Assault; Red, White and Blue; Chaos 88; and Blue-Eyed Devil. Hate rock serves as a powerful tool for hate groups seeking recruits among the hundreds of fans professing to despise African-Americans, Jews, gays, immigrants and other minorities.

A group called “The Remnants,” sometimes known as the “Avis Mills Church,” is located in Salem, Camden, Gloucester and Cumberland counties. Members believe they will be the remnant of society that will survive RAHOWA. This is a common dogma of the Christian Identity religion, which espouses racist and anti-Semitic views. Adherents are preparing for a war against an incipient worldwide, centralized government (a so-called “New World Order”) that they contend will decimate the white race at the behest of non-white populations. They refuse to recognize higher levels of government, such as state taxing or motor vehicle authorities. In the tradition of *posse comitatus*, they establish their own “private courts” at the county level and ignore peace officers enforcing laws they find disagreeable.

The white separatist group National Alliance, based in Hewitt, New Jersey, and neo-Nazi groups have given speeches in Sussex and Passaic counties. The Ku Klux Klan held recruitment drives in Ocean and Gloucester counties during the summer of 1999 and its Knights of Freedom cell is based in Eatontown and Ocean City. A racist hate group, Day of the Rope, operates out of Berlin.

The Anti-Defamation League reported that bias incidents against Jews rose 16 percent in New Jersey from 1997 (197 incidents) to 1998 (229 incidents). In 1998, anti-Semitic vandals struck at least 166 times in New Jersey, an increase of 25 percent from 133 incidents in 1997. In August 1999, the State Police released the 1997 Bias Incident Offense Report, which showed that New Jersey law enforcement agencies reported 807 bias crimes stemming from 728 incidents. That represented a 22 percent decline from 1996. However, Jews were targeted more than any other religious group, accounting for 208 offenses reported.

Whether viewed as increasing or decreasing, how much of New Jersey’s bias-related incidents may be attributable to the spread of online hate messages remains a matter for debate. Hard core bigots,

disaffected loners and youths lacking in self-esteem succumb to such messages and act out in destructive and violent ways. Cyberspace has permitted propaganda hostile to victim groups to proliferate. This vastly increases the opportunities for incitement to destructive action.

The Internet facilitates mass dissemination of slick propaganda via Web sites accessible to millions. It provides a method for rapid, confidential communication among members and sympathizers of hate groups. Meanwhile, it creates a "virtual community" of like-minded believers scattered around the country. The Internet also permits "audio-on-demand" — digitized versions of speeches or broadcasts available anytime the user wants to listen. Several Web sites also publish online versions of notorious books and videos.

The Internet is the first mass medium that operates without any significant moral, political or economic governor. With cyberspace now readily available to ordinary people, the cost of reaching a mass audience is insignificant. As a result, hate Web sites do not experience the regulatory effect of a market where unappealing products cannot bear the cost of continuing in business.

Five years ago, if a racist group wanted to get its message out, its members had to struggle financially, find a sympathetic printer, and work long hours compiling and editing, just to produce a pamphlet that might reach a few hundred people. Then, in March 1995, a former Klan leader created Stormfront, the first white supremacist site on the Web. Since that time, accessing the Internet and creating Web pages has become significantly cheaper and less technologically demanding. Today, a lone racist can quickly pull down copy from other sites, package it using high-quality photographs and graphics that are already available on the Internet, and create a Web page that is accessible worldwide. Often no financing at all is required.

Tallies of the number of Web sites involving violence and hate vary widely, depending on how those sites are defined. There is a lot of “churn” — sites closing down and reappearing at different addresses or in different forms.

Brian W. Youngblood, Internet Information Specialist for the Intelligence Project of the Southern Poverty Law Center, testified that Center figures, released in February 1999, showed an increase in the number of active hate Web sites from 163 in 1997 to 254 in 1998. He added that the number of those sites presented as an activity of a group increased from about 80 to 121. Holocaust denial sites and "patriot" group sites were not included in the figures, which also were limited to sites based in America.

Mark Weitzman, Director of the Task Force Against Hate at the Simon Wiesenthal Center, testified that his organization, selecting

extremist sites with broader criteria — including anti-Catholic, homophobic, abortion provider harassment, etc. — has counted more than 1,000. This does not include a multitude of other extremist communiqués appearing in youth-oriented chat groups.

Hate groups used computer bulletin boards to communicate in the late 1980s. Now the Internet offers a much larger virtual world in which they easily may appeal to the uninitiated. Unsolicited e-mail — "spam" — increasingly is used to send intimidating hate messages to unsuspecting victims and to recruit new members. Extremist hackers break into the e-mail accounts of innocent parties and use them to forward hate spam.

Many of the new Web sites and chat groups are aimed directly at children or teenagers, including upper-middle-class youth in the suburbs. In particular, the hate groups target high school outcasts because such students may be loners seeking an identity. Indeed, white supremacist Benjamin Smith, who in July 1999 killed an African-American and a Korean-American and wounded nine other Jews, Asians and blacks before killing himself, grew up in affluent Chicago suburbs. Smith had been a member of the East Peoria-based World Church of the Creator, which had touted its intolerance message on a Web site with separate pages luring small children with racist coloring books and targeting teenagers and women.

High technology provides several advantages for extremists. Encrypted messages, chat-room exchanges, e-mail and propaganda on Web sites all give racists an empowering sense of community. Even lone racists, with no nearby sympathizers, can feel they are part of a movement. Brian Levin, Director of the Center on Hate and Extremism, testified that cyberspace gives hate messages "a veneer of credibility." He added, "When you see something in color on a … monitor, … [i]t also suggests there might be more people behind it than there actually are."

Free encryption technology makes secure communication among group members easy, permitting them to organize and plot illegal activities in private. Where such secret codes were once easily breakable, new technology makes them far more formidable barriers to law enforcement detection.

Web sites give hate groups the ability to raise revenue as never before. Racist musical groups, whose recording sales were formerly promoted solely to insiders via constricted-circulation magazines, now reach wide new audiences by using the latest digital compression tools to offer quick downloading of their audio tracks off the Internet. This has stimulated the growth of labels, such as Resistance Records, that produce music appealing to white supremacists and other extremists.

The Internet offers a wealth of information to assist those inclined to express bigotry through violence. Such material ranges from instructions on building ammonium nitrate bombs to methods for converting semi-automatic weapons into full automatics.

Extremists may pirate seemingly innocuous online material and easily pervert it to enhance their own hateful messages. Mark Weitzman described how a professor in Michigan put an English translation of the children's book, *The Poison Mushroom,* on his county college Web site in order to demonstrate its use as a propaganda device by the Nazis from 1932 to 1945. An extremist Web site downloaded illustrations from the book containing unflattering color caricatures of Jews and used them to indoctrinate children with anti-Semitism. In another example provided by Mr. Weitzman, a hate site "awarded" itself a major ISP's "top five percent" designation. The ISP was reluctant, according to Mr. Weitzman, to remedy the misuse of its award because the ISP was based in the Northeast and the offender was in California. The ISP did not want to incur the expense of a distant lawsuit.

The Holocaust is the historic event that resulted in the mass murder of six million Jews, and five million others, at the hands of the Nazis and their collaborators in Europe during the period 1933-45. Holocaust deniers' propaganda insinuates subtle but hateful anti-Semitic beliefs about Jews as exploiters of non-Jewish guilt and as controllers of academia or the media. Steven E. Some, Chair of the New Jersey Commission on Holocaust Education, testified, "[C]hildren do not have that ability to discern the differences between legitimate research sites on the Internet and … illegitimate sites …."

Mr. Some cited a recent instance in which a New Jersey teacher had his class conduct a mock trial of Adolph Hitler to fulfill the school's Holocaust education curriculum. The teacher instructed his students to use the Internet in their research but did not pay careful attention to the search results. Mr. Some lamented that, as a consequence, the students' Internet inquiries led to the mock trial's acquittal of Hitler for genocide. He added that the students were taken in by the scholarly façade of Web sites where deniers "are masking themselves as legitimate sources of information on the Holocaust."

CROSSING THE LINE FROM HATE SPEECH TO HATE CRIME

Our society, which cherishes freedom of speech, tolerates even obnoxious utterances. Society need not, however, condone hurtful conduct accompanying such expression. A major concern about all the extremist activity on the Internet is whether it inspires violence. Brutality motivated by antagonism toward minorities or the opposite sex is intolerable. As delineated by the Rev. Martin Luther King, Jr.:

"Morality cannot be legislated, but behavior can be regulated. Judicial decrees may not change the heart, but they can restrain the heartless."

Bias crime victims are targeted because of race, creed, ethnicity, sexual orientation, gender or handicap. Perpetrators assault those of different races, desecrate cemeteries, bash gays, burn crosses in people's yards, vandalize synagogues, spray hateful graffiti, and threaten multi-racial couples.

Bias crimes are more likely to involve excessive violence, multiple offenders, randomness, irrationality and violations of victims' civil rights, including travel, housing, schooling and employment. In addition, bias crimes generally are more likely than other types of crime to traumatize an entire community.

Meanwhile, those who harbor animosity toward the opposite sex use cyberspace as a tool to harass or intimidate victims more effectively. The Prejudice Institute (www.prejudiceinstitute.org), a Baltimore-based, non-profit, non-partisan hate-crime research and education organization, reported in 1998 that sexual harassment of women on college campuses by e-mail was four to five times more common than racial or ethnic harassment.

Cyberspace can be rough around the edges, frequented by many users who sometimes fail to appreciate social propriety. As a result, common online activities include rude behavior such as "flaming" (unleashing a hyperbolically nasty attack) and "trolling" (making provocative statements in order to get an angry reaction). Extremist groups and individuals take full advantage of their First Amendment rights in such a milieu. Most of their Web sites do not blatantly promote violence, but they provide enough misinformation to rationalize violent action by some of the sites' adherents.

In response to a lawsuit filed in New Jersey in late 1999, a federal court enjoined a Hazlet couple from accessing the iVillage.com Web site. The defendants allegedly posted thousands of obscene, vulgar and threatening messages in an attempt to shut down a breast-feeding discussion board. The lawsuit, which seeks several million dollars in damages, alleges that the defendants posted some of the offending remarks under more than 70 user names and in at least one case appropriated the screen name of a legitimate iVillage.com user. A state judge in New York approved a subpoena for records from the defendants' ISP, which identified them as the senders of the messages. The attorney for the plaintiff, iVillage, opined that the civil process permitted a swifter halt to the conduct than referring the matter to law enforcement officials.

To deal with the violence accompanying expressions of hate, the Anti-Defamation League pioneered special criminal laws. In *Wisconsin*

v. Mitchell, 113 *S.Ct.* 2194 (1993) the United States Supreme Court unanimously held that the First Amendment of the United States Constitution does not prohibit a state from providing enhanced punishment for a crime based on the actor's discriminatory purpose in committing the crime. In *State v. Apprendi,* 159 *N.J.* 7 (1999) New Jersey's Supreme Court validated this state's hate crime law. The statute, *N.J.S.A.* 2C:44-3(e), allows years to be added to a defendant's sentence if the judge determines by a preponderance of the evidence that the criminal acted "with a purpose to intimidate … because of race, color, gender, handicap, religion, sexual orientation or ethnicity." The defendant's appeal in *Apprendi* was argued before the U.S. Supreme Court in March 2000.

New Jersey first adopted hate crime legislation in 1981 and expanded its coverage in 1990 by passing the Ethnic Intimidation Act, which increases the penalties for any crime committed with a purpose to intimidate an individual or group because of race, color, gender, handicap, religion, sexual orientation or ethnicity. The law also affords civil remedies to victims, including punitive damages. Although New Jersey's stringent law enforcement reporting requirements cause it to lead the nation in the per capita reporting of bias crime, most bias crimes in the state involve harassment, terroristic threats and criminal mischief in which the Internet is not the vehicle. However, in 1998, the New Jersey Division of Criminal Justice successfully prosecuted a notorious case that involved the Internet in *State v. Gancarz, et al*. In that matter, young adults carved a 70-foot swastika in a cornfield and continuously harassed African Americans in Burlington County. They communicated with each other and solidified their prejudiced group identity via the Internet.

In March 2000, the Somerset County Prosecutor's Office and the State Police investigated a threatening note linked to a now-defunct Web site allegedly created by students at a South Bound Brook middle school. At least one student was suspended, and authorities were trying to locate the computers used to set up the Web site. The note displayed two swastikas and racial slurs. It threatened by name to "take out" two boys and to "get" one of them and "lock him up like a slave."

In 1998, Pennsylvania Attorney General D. Michael Fisher sought injunctive relief against those associated with White Power World Wide, an offensive Web site created by a white supremacist. Others sued included the Internet service provider (ISP) and the company that registered the domain name. Mr. Fisher chose not to prosecute the white supremacist for alleged terroristic threats and harassment. He accomplished his goal of removing the offensive material, because the Web site shut down. It is not known whether the white supremacist or his ISP removed the site. Mr. Fisher moved ahead with the lawsuit anyway. Although the ACLU labeled the action an unconstitutional prior restraint against free speech, a court in mid-1999 enjoined the site

from appearing on the Web. The court found that a posted disclaimer discouraging acts of violence was ineffective in the face of specific posted threats.

Mr. Fisher's lawsuit objected to three entries that appeared on the Web site. One statement warned that people such as a named and pictured anti-hate activist would be "hung from [her] neck from the nearest tree or lamp post." The Web site also showed a computer-generated image of the activist's office exploding.

A bigot legally can put all sorts of racist invective on a Web site, but he cannot simply threaten to kill someone over the Internet. When deciding what is protected speech, we must consider the likelihood that a particular statement will incite another to "imminent lawless action." That is the standard set forth in 1969 by the U.S. Supreme Court in *Brandenburg v. Ohio* to define the limits of protected speech. The Internet complicates the analysis, however, because it is a relatively emotionless medium. Messages in cyberspace may be deemed too remote in time and space to incite an immediate illegal reaction. However, a threat is a threat, and just because the Internet is a new medium should not insulate an offender from liability.

On September 20, 1996, a student who had flunked out of the University of California at Irvine (UCI) sent an anonymous, profanity-laced message to 59 Asian students. The message told them that if they did not "get the ____ out of UCI," he would "hunt all of you down and Kill your stupid asses." The message continued, "I personally will make it my life career to find and kill everyone of you personally." An administrator at the computer lab quickly collared the former student, who carelessly included his own name (the only non-Asian one) on the list of recipients so that he could receive replies. The former student confessed to sending two such messages. School officials banned the former student from UCI property, but the incident was not reported outside the University community for several days. Local police declined to prosecute, but the FBI heard about the case and it became the first federal prosecution of a hate crime in cyberspace to go to trial.

The former student was prosecuted under an obscure 1960s civil-rights statute aimed at segregationists preventing black children from entering public schools in the Deep South. The law seeks to punish anyone who "by force or threat of force attempts to injure, intimidate or interfere with … any person because of his race, color or national origin and because he is or has been enrolling in or attending any public school or public college." The jury convicted the former student of one of two counts, and the judge sentenced him to a year in prison.

On February 2, 1999, an anonymous federal civil jury in Portland, Oregon, awarded $107 million in damages to Planned Parenthood and four physicians against the American Coalition of Life Activists and Advocates (ACLAA) of Portland and its officers. The defendants had distributed wanted posters naming abortion providers and had submitted a list of the providers, their employees and spouses, judges and pro-choice advocates to a Georgia-based Web site called “The Nuremberg Files,” which posted it as a high-tech “hit list.” The list included home addresses, photographs and license plate numbers of the providers, and, in at least one case, the names of their children and the schools they attended. The site’s operators drew lines through the names of those killed. Those who were wounded were grayed out.

The ACLAA case was brought under the federal RICO statute, 18 *U.S.C.* §1961 *et seq.*, and the Freedom of Access to Clinic Entrances Act of 1994, 18 *U.S.C.* §248, which makes it a federal crime to use force or threat of force against anyone seeking or providing an abortion. The case is on appeal. In charging the jury, the judge said the Web site should be deemed threatening if it could be taken as such by a "reasonable person." Some experts believe this might not meet the Supreme Court’s incitement test because it may lack imminent risk of harm. The Supreme Court eventually will be called upon to refine this standard in the context of a medium capable of mobilizing a host of zealots with a single keystroke.

Finding the line between protected and unprotected expression is a delicate, fact-sensitive task. The Nuremberg Files’ ISP took the site off-line for violating appropriate use policies. Later, the federal court in Oregon enjoined ACLAA from publishing the posters and submitting information to the Nuremberg Files for publication if such publication was made with an “intent to harm.” The court concluded that the defendants had crossed the line from idle threat, hyperbole and the like, which the First Amendment protects, to a threat that could be enjoined and fined, because of the context of the campaign of violence waged against abortion providers.

On August 20, 1998, an individual posing as "John Blau" posted information on the Internet indicating that Missouri FreeNet, an ISP, would post information about law enforcement officers, such as photo, name, address, phone number, and vehicle identification. Contributors were asked to "HELP EXECUTE" a law enforcement officer by contributing to the "LEO Information Project." In other postings, "Blau" openly urged the execution of law enforcement officials. When concerned citizens contacted Missouri FreeNet, they were told that "Blau" would be permitted to continue the "LEO Information Site," minus the "HELP EXECUTE" quote. Missouri FreeNet also confirmed that "Blau" is its system administrator.

Hate groups and their leaders have been found liable in civil lawsuits for the violent actions of members or those they purposely

orchestrated or negligently encouraged. The Southern Poverty Law Center has taken the lead in bringing such lawsuits.

In 1987, a $7 million judgment bankrupted the Alabama-based United Klans of America for its connection to the lynching of a 19-year-old African-American named Michael Donald. In 1990, an Oregon jury rendered a $12 million verdict against the Fallbrook, California-based White Aryan Resistance and its leadership for promoting the killing of a young Ethiopian immigrant named Mulegetta Seraw. In 1994, the Church of the Creator — predecessor of the virulently racist World Church of the Creator — lost a million-dollar lawsuit under a Florida state civil RICO law for its part in the murder of a young African-American Gulf War veteran, who was killed by a Church "reverend." In mid-1998, two Carolina Klan groups were held liable for $21.5 million for their connection to the arson of two black churches.

Brian Levin testified that successful civil lawsuits have led hate groups to adopt a new strategy of "leaderless resistance," mimicking a type of guerrilla warfare where individuals or autonomous cells independently undertake violent acts against common enemies without relying on a centralized command and control structure. The concept has been promoted on the neo-Nazi Stormfront Web site and in racist books like "The Turner Diaries" and "The Vigilantes of Christendom." "Vigilantes" misinterprets the Bible to encourage lone wolves to anoint themselves "Phineas Priests" by committing violence. The strategy guided a convicted felon who robbed banks and attacked abortion clinics. "The Turner Diaries," a novel revered by white supremacists, has a protagonist who blows up a federal building and randomly targets minorities for murder. The "Diaries" and "Homemade C-4," both readily available for free on the Internet, allegedly inspired the bombing of the federal office building in Oklahoma City in 1995. The convicted murderer of James Byrd in Jasper, Texas, allegedly explained to his cohorts, before they dragged the hapless Mr. Byrd to death behind a pick-up truck, that he was "starting the 'Turner Diaries' [revolution] early."

Although the First Amendment to the U.S. Constitution severely limits government censorship, private Internet Service Providers (ISPs) can eliminate anything they deem offensive from their systems. While a few police the content of chat rooms and Web sites, others are philosophically opposed to playing the role of censor or consider it to be an exercise in futility. Most ISPs consider themselves to be mere conduits to the Internet. Moreover, if an ISP shuts down discussion groups espousing racism or intolerance, several more may, in short order, pop up on its network of sites. Web sites that are shut down seem to have little trouble finding new ISPs.

ISPs express concern that if they were to start regulating content, it would open the door to all kinds of liability problems. (But see §230 of the Communications Decency Act, which shields ISPs

from liability.) Still, many ISPs have developed a range of policies, delineated in terms of service agreements, that define what is and is not appropriate. Although they maintain they cannot possibly monitor all members, in some cases numbering in the millions, these ISPs do respond to complaints from both members and outsiders, including anti-hate groups such as the Anti-Defamation League. By strictly enforcing carefully drawn terms of service agreements, ISPs could stop hate from spreading without the government having to violate free speech rights.

CONTROL ORGANIZATIONS, PROGRAMS AND LAWS

Solutions to cyberspace bias and hate are arduous in a society that venerates freedom of speech. As observed by Oliver Wendell Holmes, “The mind of the bigot is like the pupil of the eye; the more light you pour upon it, the more it will contract.” It follows that prevention and education strategies to combat bias and hate need to be expanded at the national, state and local levels. We must continue to educate teachers and law enforcement. All children must be told about the dangers that lurk on the Internet. Parents and guardians must learn how to protect their children and help them to protect themselves, especially with critical thinking skills. While these laborious but necessary tasks are being accomplished, law enforcement must enforce vigorously laws prohibiting violent action arising from prejudice. Several private and public organizations currently take part in monitoring, education and enforcement involving online bias activities.

Government censorship would not work in cyberspace, even if it were constitutional. The problem is not intractable, however, because centers of reason have shed light on the situation before the whole of the Internet could be compromised. Corporate leaders, especially, can accelerate this sanitizing process by implementing standards for what they will allow on their systems and by helping to provide effective forums for positive forces. Jordan Kessler, Research Analyst for the Anti-Defamation League, testified that Bell Atlantic stands out as a corporation devoted to countering hate. He praised the company’s funding of civil rights Web sites and its former CEO’s speeches against online hate. Such efforts enable the Internet to foster tolerance far better than it advances hatred. In this way, the community can relegate hate messages to society’s margins.

OFFICE OF BIAS CRIME AND COMMUNITY RELATIONS

The New Jersey Office of Bias Crime and Community Relations is responsible for the statewide prosecution and monitoring of hate crime. It is the only statewide office in the nation dedicated solely to addressing hate crime. Created in 1992, it serves as a central

resource for hate crime information and gives national leadership on hate crime policy and initiatives. Through the New Jersey Bias Crime Training Program, the Office trains law enforcement officers in the investigation of bias crime. It also offers a wide array of other programs in hate crime awareness and prejudice reduction including the Prejudice Reduction Education Program (PREP), a curriculum that teaches students about hate crime prevention.

Among the training initiatives offered to address bias crime and its underlying causes is Hate on the Internet, a one-hour program. Begun in the fall of 1999, the program teaches educators and families how to protect young people from the influence of hate groups and their Web sites. Approximately 2,500 teachers and parents from across New Jersey have attended the program since its inception. The Office of Bias Crime and Community Relations also sponsors the New Jersey Bias Crime Victims' Support Service, 1-800-277-BIAS (2427), a program that helps bias crime victims through telephone referrals to law enforcement agencies, human service providers and trained volunteers. The office also monitors hate Web sites throughout the country and shares information with New Jersey law enforcement agencies as they investigate hate crime activity.

DIVISION ON CIVIL RIGHTS

The Division On Civil Rights (Division) enforces New Jersey's Law Against Discrimination (LAD). It is unlawful under the LAD for anyone to circulate or publish any advertisement for employment or housing that discriminates against individuals because of race, color, creed, national origin, gender, marital status, or any other category protected by the LAD. *N.J.S.A.* 10:5-12; *N.J.A.C.* 13:9 and 13:11. Therefore, employers, employment agencies, homeowners, landlords and real estate brokers who advertise on the Internet should ensure that employment and housing ads contain no language that would tend to discourage individuals from responding because of their membership in a protected category.

The Division is taking steps, in conjunction with other Law and Public Safety agencies, to monitor ads on the Internet to ensure that they do not contain the discriminatory language prohibited by the LAD. If a violation of the LAD is discovered, the Division will file an administrative complaint against the perpetrator and will seek statutory penalties and compensatory damages. Users who suspect that an Internet posting may violate the provisions of the LAD should contact one of the five Division offices, using the telephone numbers appearing on the Division's Web site at www.state.nj.us/lps/dcr. This site also provides a detailed description of the protections afforded by the LAD and the services provided by the Division. Users who desire more information or technical assistance on how to make sure their ads comply with the LAD should contact the Division's Bureau of Prevention

and Citizen's Rights at (609) 292-2918.

The Attorney General's Internet Working Group is in the process of developing an extensive, interactive Web site which will be an important resource for those seeking information on recognizing and combating online discriminatory practices and hate and bias issues.

ANTI-DEFAMATION LEAGUE

The Anti-Defamation League (ADL) of B'nai B'rith, founded in 1913, defends free speech and does not condone banning hate speech in cyberspace. Instead, it promotes positive responses, believing that the best way to combat hateful speech is with more speech. Its Web site is www.adl.org. An ADL report, *High-Tech Hate: Extremist Use of the Internet* (1997, 86 pages), documents online racists and explores hate Web sites. Other resources include a *Guide to Hate Crimes Laws*, a hate crime training video, and *Blueprint for Action*, developed for the November 10, 1997, White House Conference on Hate Crimes.

In libraries and bookstores, material can be labeled and organized so as to enable parents to exercise discretion about what their children see. Blocking software attempts to afford parents the ability to exercise similar discretion over the Internet. In cooperation with The Learning Company (TLC) of Massachusetts, the ADL in 1999 released filtering software using the technology of TLC's CyberPatrol® software. Entitled HateFilter™, this software blocks access to Internet sites that, the ADL believes, promote hate. Since the ADL seeks to balance the right to free speech with the need to fight hate speech, it does not market HateFilter™ to schools, libraries or public facilities. The software serves primarily to allow parents to control their children's computer use. It refers a blocked user to an ADL site that explains why a site was blocked. HateFilter™ also prevents unauthorized users from using racist or anti-Semitic chat lines and newsgroups, whose effectiveness as a means of spreading hate over the Internet rivals Web pages.

As is the case with child pornography and pedophilia over the Internet, screening software is not a panacea to the problem of online bias and hate. According to Arthur Wolinsky, a New Jersey-based expert in online safety for school children, students need exposure to critical thinking and media literacy skills in order to determine what is true and what is not. Mr. Wolinsky elaborated:

> When it comes to hate groups and extreme views on the Internet, filtering is NOT the solution. Students will eventually come in contact with this type of information. If they have been "protected" from it by filters, they will be at the mercy of the hate groups when they finally do come in contact with them elsewhere. If these hate and extremist sites are used within the

context of media literacy lessons, they will be able to deal with the material whenever and wherever they come in contact with it.

In mid-1999, the ADL formed a task force to examine the recent explosion of electronic hate expression. The task force is comprised of representatives of ISPs, educators, law enforcement officials, prosecutors and community leaders.

CENTER ON HATE AND EXTREMISM

The Center on Hate and Extremism was established at Richard Stockton College in Pomona, N.J., in August 1996. In the summer of 1999, both the Center and its Director, Professor Brian Levin, relocated to California State University at San Bernardino.

One of the first such programs in the United States, the Center analyzes trends and legal and criminological aspects of expressions of hate, extremism and terrorism. It provides legislative testimony, *amicus curiae* briefs and law enforcement training. It is non-partisan and has an Advisory Board. It has developed a Model Hate Crime Statute.

In 1995, Professor Levin helped the New Jersey Attorney General's Office implement a federal pilot program that teaches law enforcement officers how to handle bias crimes. He worked on the project with the Office of Bias Crime and Community Relations in the Division of Criminal Justice.

SOUTHERN POVERTY LAW CENTER

Founded in 1971, the Southern Poverty Law Center (SPLC), based in Montgomery, Alabama, operates a Teaching Tolerance program and also keeps close tabs on hate groups and their activities. The SPLC's Web site is located at http://splcenter.org. The SPLC's Intelligence Project publishes a quarterly *Intelligence Report*. The organization regularly conducts training sessions for police and community groups.

The SPLC created Klanwatch in 1981. It tracks the activities of over 500 hate groups. The SPLC established a Militia Task Force in 1994. It monitors 523 militias and other groups espousing extreme anti-government views. Six months before the April 1995 Oklahoma City bombing, the SPLC warned the U.S. Attorney General that the new mixture of armed groups and those who hate was a recipe for disaster.

NEW JERSEY COMMISSION ON HOLOCAUST EDUCATION

The New Jersey Commission on Holocaust Education, www.state.nj.us/njded/holocaust, (an offshoot of the New Jersey Advisory Council on Holocaust Education) was created by statute in 1991 to recommend curricular material on the Holocaust and other genocide. See *N.J.S.A.* 18A:4A-1 *et seq*. In 1994, the law was amended to require every board of education to include instruction on the Holocaust and genocide in the curriculum of all elementary and secondary school pupils. The law provides:

> The instruction shall enable pupils to identify and analyze applicable theories concerning human nature and behavior; to understand that genocide is a consequence of prejudice and discrimination; and to understand that issues of moral dilemma and conscience have a profound impact on life. The instruction shall further emphasize the personal responsibility that each citizen bears to fight racism and hatred whenever and wherever it happens.

The Commission on Holocaust Education sponsors seminars to train teachers on how to use the Internet properly for class projects. It makes resources available to the education community and assists three dozen Holocaust/genocide resource centers and demonstration sites located at colleges and school districts around the state. In addition, the Commission organizes an annual summer field trip for about 30 teachers to spend 12 days in Eastern Europe and Israel learning about the Holocaust. Corporate sponsors fund much of the cost of the trips.

SIMON WIESENTHAL CENTER

The Simon Wiesenthal Center, based in Southern California (www.wiesenthal.org), distributes a CD-ROM called “Digital Hate 2000,” listing hundreds of extremist Web sites. When the Center started tracking such matters in April 1995 at the time of the bombing of the Oklahoma City federal building, it identified just one hate Web Site. The Center has a CyberWatch Survey project, a Task Force Against Hate and a hotline.

Encouraged by the example of CNN and some newspapers denying a forum to certain paying advertisers, the Wiesenthal Center wrote to thousands of Internet service providers (ISPs) offering a voluntary code of ethics. Only a handful responded. Although ISPs are in the business of selling space for advertising, they have no obligation to take money from all those interested in putting up Web sites. Most ISPs say they operate like common carriers and are obligated to

transmit whatever messages come into their systems. Some ISPs have catered to extremists.

The Center urges customers to complain if their ISPs allow hate material on the sites that they host. It has criticized online auctioneer eBay for permitting the sale of Nazi paraphernalia and collectibles over its Web site. It also lambasted Internet booksellers for carrying books such as Adolf Hitler's *Mein Kampf* and a biography of Nazi leader George Lincoln Rockwell.

HATEWATCH

HateWatch, a non-profit organization founded and directed by David Goldman, a full-time law librarian, originated with a Harvard University Library guide called "A Guide to Hate Groups on the Internet." Although it has sparked controversy with those who oppose drawing attention to hate groups, HateWatch, in an effort to "drag these people out of the shadows," posts information about a variety of such groups on its own Web site, located at www.hatewatch.org. HateWatch also lists ISPs that do not permit hate-spouting Web sites.

Mr. Goldman reported that economics is forcing a decrease in sophistication and originality of hate material on the Internet. He noted that many "orphan" hate-based Web sites lie dormant — without updates or development. Others are low in quality and not very persuasive, according to Mr. Goldman. He added that extremists are now more likely to participate in chat groups. While concluding that the activity of organized groups has leveled off, Mr. Goldman maintains that harassing or threatening e-mail has increased.

HateWatch encourages customers to report hate traffic to their ISPs. It also encourages people to start their own anti-hate Web sites and is developing free software that will enhance such Web sites so that they will better serve visitors.

OTHER ANTI-EXTREMIST ORGANIZATIONS

The following organizations have programs and Web sites to counter the activities of extremist groups and to promote diversity and human rights.

InterGOV International (www.intergov.org) is a central meeting place where Internet enthusiasts can develop internationally accepted standards for the online community and offer services to protect children and to police the integrity of the Internet. The organization recommends that victims of "flaming" notify the appropriate chat room administrator and ISP immediately.

The Center for Democratic Renewal was founded in 1979 as the National Anti-Klan Network. Its Web site, hosted by the Institute for Global Communications (IGC), is www.publiceye.org. IGC also sponsors "Not In Our Town" (www.igc.org/an/niot), a national movement against hate crimes.

The Leadership Conference on Civil Rights, located at www.civilrights.org, counters prejudice, extremism and hate crime in America. Facing History and Ourselves National Foundation, Inc. (www.facing.org) promotes study of the historical development and lessons of the Holocaust and other examples of genocide.

HACKING

THE PROBLEM

Unauthorized accessing of computer systems — sometimes called hacking, industrial espionage, intrusion, penetration or cyber-terrorism — exhausts massive private and public resources. Furthermore, such conduct threatens public confidence in national defense, the ability of strategic industries to function and the integrity of the cyber-marketplace.

An unsuspecting computer user can acquire software "viruses" by downloading "infected" programs from Web sites or opening e-mail attachments containing viruses. One of the newest viruses, BubbleBoy, can intrude into a victim's system if he or she merely previews the list of incoming e-mail messages using Microsoft Outlook. Fortunately, it is not harmful and is easily eliminated. If not removed or fended off with regularly updated anti-virus software, many other computer viruses can wreak havoc within computer systems, even erasing every bit of data on the hard drive. The typical virus cannot, however, harm hardware, including the hard drive itself.

American companies spent almost $6.3 billion on computer security in 1997, according to DataQuest, a research firm. This mammoth expense is expected to grow to $13 billion by the year 2000.

The San Francisco-based Computer Security Institute (CSI) (www.gocsi.com) is a trade organization that has assisted and trained information system professionals since 1974. For the last five years, in cooperation with the Computer Intrusion Squad of the FBI's San Francisco Office, it has released the results of an annual Computer Crime and Security Survey. The survey results released in 2000 found that 70 percent of 585 participating U.S. corporations, government

agencies, financial institutions and colleges reported serious computer security breaches within the previous year. System penetration by outsiders, unauthorized access by insiders and theft of proprietary information all rose from the period covered by the survey released in 1999. Almost 90 percent of the security professionals who answered the survey detected a security threat. Only 42 percent of the companies affected estimated the amount of damage suffered. The total came to $266 million, more than double that of 1999.

By the end of 1999, the FBI had 800 pending cases involving computer hacking and intrusion. This compares with 200 cases just two years earlier.

Perhaps society's greatest anxiety stems from concern about terrorist groups and foreign governments bringing down defense or economic infrastructures by using "information warfare." In such scenarios, hackers would disable the computers that control the nation's telephone system, banks and stock exchanges, as well as the power grid or the pipes that pump gas, oil and water around the country. The integration of America's public and business computer networks increases the risk that problems affecting one system also will affect others, thus placing the nation's computer-based critical infrastructures at increased risk of severe disruption. Indeed, the United States itself takes advantage of vulnerability in its enemies' computer systems. On October 7, 1999, the Chairman of the Joint Chiefs of Staff acknowledged that the U.S. military used offensive information "weapons" against Yugoslavia during NATO's Kosovo campaign air war.

Less dramatic intruder activity can still have far-reaching negative consequences for individual businesses. For example, cyber-extortion occurs when an intruder plants a "logic bomb" on a computer that might disrupt a system responsible for processing customer transactions. The extortionist tells the company that unless he receives money by a certain time, the system will be disabled.

According to Malcolm Skinner, Marketing Manager at Axent Technologies, external hacking is growing by an alarming 36% each year. Hackers make money through raiding bank accounts, credit card fraud, telephone call selling, product/service fraud, espionage (stealing and destroying information in government and business computers) and hostage-taking/extortion (threatening to unleash viruses).

In February 2000, computer hackers using sophisticated "distributed denial of service" attacks, disrupted Web sites operated by several leaders of the electronic marketplace, including Yahoo!, eBay, Amazon.com, Buy.com, Time Warner's CNN.com, Etrade, Microsoft's MSN.com and ZDNet. The perpetrators flooded victim sites with massive amounts of bogus message material, effectively closing them to routine

traffic the way a telephone switchboard could be swamped with too many calls. Although no consumer data was compromised, the disruptions jarred consumer and investor confidence in e-commerce, causing high-tech stocks temporarily to register sizeable losses in value on stock exchanges.

In April 2000, following a joint investigation by the FBI and the Royal Canadian Mounted Police, Canadian authorities charged a 15-year-old boy, using the computer name “Mafiaboy,” with two counts of mischief for disrupting CNN’s Internet site. The boy allegedly used software “tools,” readily available on the Internet, for denial of service attacks that he boasted about in chat rooms frequented by hackers. He faces a maximum sentence of two years in a juvenile correctional center and a $650 fine.

Hackers have even turned security tools, such as network firewalls, against organizations to mount denial of service attacks. A firewall is a system of hardware and software configured to prevent outsiders from accessing and using a computer network and any other resources connected to the network.

Also in February 2000, the Computer Emergency Response Team (CERT) of Carnegie Mellon University warned that harmless-looking Web links could, in fact, be rigged with so-called “cross-scripting” to damage, or steal information from, computers of unsuspecting Web surfers. On Web sites collecting information from customers with electronic forms hackers could interject harmful software commands to steal banking or other personal information. Web site administrators must constantly review their computer code to weed out such potential problems.

In May 2000, the so-called “Love Bug” virus and its imitators disrupted the computers of anyone who opened the attachment to an e-mail titled “ILOVEYOU.” The virus crippled private sector and government communications worldwide by clogging e-mail servers and overwriting files. It also attempted to inject another program from a Web site in the Philippines that would search computers for Internet access passwords and e-mail those passwords back to an address there. Damage estimates have run from hundreds of millions of dollars to $10 billion, mostly the result of lost productivity.

Experts agree that there is no network, Web site or system that is 100 percent secure against hackers, who have been breaking into computers over telephone lines since the late 1970s and now use the Internet. In the original sense of the word, a hacker was someone with a talent for determining how technology works and the skills to program computers to perform advanced tasks. In the more common vernacular, it has come to mean a person who attempts to intrude into, or attack, computer systems so that they will do his or her bidding. Other common terms for hackers include attacker, cracker and intruder.

Fear of unauthorized intrusion should not deter governments, individuals or businesses from taking advantage of the unlimited potential afforded by computers. For the most part people think nothing of flying, although no one guarantees that there will never be a plane crash. As long as people are satisfied that all that can be done is being done, they will continue to fly in great numbers. Similar reasoning should encourage participation in cyberspace, where a mishap ordinarily would not end any lives.

An array of security measures is available to ensure that commercial transactions over the Internet cannot be corrupted by outside parties. Secure Electronic Transactions (SET) software, developed jointly by Visa and MasterCard, reduces substantially the potential for credit-card fraud. It uses encryption technology to protect information from unauthorized viewing. When an online purchase is made, the credit card information is stored in a digital envelope, which the merchant cannot open. The merchant passes the envelope, along with its digital identity, to the credit-card company for processing.

Secure sockets layer (SSL) is a type of encryption technology that protects credit card information by scrambling it before transmission. To find out whether credit card information is secure, consumers can look at the URL for the merchant’s Web page. A secure URL page begins with the code "https" rather than "http."

Security-conscious consumers patronize Internet merchants displaying security seals, such as Web Trust(SM), created by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants. The seal assures online customers that the businesses carrying it on their Web sites adhere to standard business practices and controls and have the ability to maintain privacy and security for Internet transactions.

If someone deliberately does something injurious to a computer, chances are it is an inside job, ranging from theft of confidential information to fraud to a grudge attack. The most dangerous motive is revenge by a disgruntled employee. When something goes wrong with a system, often one of its own information technology (IT) people is responsible. Even if their own employees can be trusted, some companies may have neglected to check the backgrounds or double-check the work of outside contractors. Such internal offenders can easily render firewall, anti-virus, network analysis and host-based monitoring software protection useless. When trying to track the perpetrator in such circumstances, one has to remember that it is pointless to ask the internal offender to investigate himself. The single most important measure a company can take to ward off intrusions is to hire trustworthy employees and consultants.

David J. Goldstone, Trial Attorney in the U.S. Justice Department's Computer Crime and Intellectual Property Section, emphasized in his testimony the need to recognize inside vulnerability:

> In my experience, the cases that I've investigated with the Department of Justice, most common, and often most damaging, kinds of hackers that attack private corporations are disgruntled ex-employees, particularly ex-employees who work in the MIS [Management Information Systems] Department. There are often very few controls in the MIS Department in the way of background checks. The MIS Department doesn't conceive of itself as a security department, but it is often essential to the security of a business, particularly as we're in the information age and so much of a company's value lies in stored information. If it happens that one of the employees in the MIS Department leaves the company under unhappy circumstances, then he can have the motivation and the knowledge to shut that company down, and I've seen that happen in a number of situations. I would say that's the most common motivation for hackers in the private sector.

In one of the first prosecutions of its type in the nation, the former Chief Network Administrator of Omega Engineering Corp. was convicted in the New Jersey federal district court in May 2000 of planting a computer "time bomb" that cost the company more than $10 million. Demoted prior to being fired in 1996, the disgruntled employee stayed after regular business hours programming and testing commands that eventually would wipe out permanently all the design and production programs vital to Omega's New Jersey manufacturing operations. The "bomb" had been designed to activate automatically if a countermanding command was not received.

Although inside jobs remain an important threat, attacks against computer security from outside the victim organizations are increasing in frequency. Traditionally, internal attacks posed the greatest threat to computer networks. They accounted for about 85 percent of all attempted intrusions, while the remaining 15 percent came from external sources. However, according to survey results released in July 1998 by Internet Security Systems, 61 percent of corporate respondents suffered computer system attacks originating from inside the organization, and 45 percent of those attacks resulted in losses over $200,000. Meanwhile, 58 percent of the respondents experienced external attacks, with 50 percent of those attacks resulting in losses over $200,000. The Computer Emergency Response Team (CERT) at Carnegie-Mellon University also reported rapid growth in the number of incidents of computer security breaches: from 1,334 in 1993 to almost 4,400 in just the first two quarters of 1999.

Meanwhile, the extent of the problem is substantially underreported because private companies, shy of bad publicity, usually

want to avoid disclosure of intrusions to their systems. In a report issued on October 4, 1999, the U.S. General Accounting Office stated, “Private entities are reluctant to disclose known problems or vulnerabilities that might weaken their competitive positions or diminish customer confidence.”

The rise in penetration from external sources corresponds to the boom in global Internet connections and the rush by businesses to establish a presence on the Internet regardless of security preparedness. More and more individuals and companies are sending data across the Internet’s insecure lines. Those who entrust their important confidential information to computer files will live to regret any failure to take proper precautions to safeguard those files. In most cases, the precautions are simple, easy and inexpensive.

If hackers do disrupt a weakly protected system, it may be difficult to identify them. Hackers employ techniques, such as "onion skin" technology, to make their presence on the Internet or e-mail anonymous. They may penetrate multiple systems and “daisy chain” their attacks (sometimes called “connection laundering”) to increase the difficulty of tracing them back from their victims. They may work in tandem with other hackers and store their hacking “tools” at remote secondary sites in different states or countries. Interpol, the international police agency, estimates there are 30,000 hacker-oriented Web sites.

Joseph G. Degnan, a Special Agent with the Naval Criminal Investigative Service responsible for New York, New Jersey and Pennsylvania, testified about the typical hacker and how he poses a threat to unprepared computer operations:

> I can tell you a hacker is … a 14- to 25-year-old student. He is isolated, technologically advanced. His parents don’t care what he does at night sitting up in his room on his computer system. But there are also people that are very good at speaking, [social engineers who] can gain access to information that you shouldn’t be giving out over the phone. So you need to educate and make people aware of it, businesses and government entities and everybody else.
>
> That’s why I’m going out and speaking to defense contractors in the State of New Jersey, so that they are aware that somebody is very interested in the information that resides on their computer systems, so that they properly protect and safeguard the information, so that it is not downloaded or given away for free to somebody that either asks over the telephone or dials into the Web page.

Hacking offers the thrill of joy riding. It is like a game of high-speed chess where the skillful seek bragging rights in the hacker community. The hacker mentality, which used to be "look but don't touch" and included help from "white hat" good-guy hackers who pointed out computer systems' weak points, has expanded to more sinister realms. It increasingly involves the quest for money or even "cyber-terrorism," such as crashing a system.

Edward F. Skoudis, Technical Director and Program Manager in Global Integrity's Consulting Services Division, testified that hacking threats are extremely diverse:

> I think we have got to be very careful with this concept of creating a hacker profile or defining in law what is hacking. … [T]here are so many different individuals in so many different walks of life that could do this kind of thing.
>
> One thing that we caution our customers about is to not assume that you will be attacked or hacked by a pimple-faced kid, because that usually makes you underestimate your adversary. Yes, the pimple-faced kids are very good, but there also may be some extortionist or some organized crime type person trying to exact a financial target rather than just cause annoyance. So you don't want to underestimate your adversary, and I don't think you can very easily classify what is a hacker.

Wannabe hackers obtain their skills in many ways. Much of the how-to information and software tools that automate the hacking process comes free-of-charge from the many online sites hosted and frequented by hackers, rather than from underground sources. Mr. Goldstone described why the learning curve to achieve basic hacking capability is not very great:

> I have seen Web sites with pages and pages of software programs, and you don't even need to learn the ABCs of hacking. All you need to do is download the software program, point it at the computer that you would like to attack, and let the program do the work for you. So you don't have to be a computer genius to be a very effective hacker.

Some hackers abuse software available for free on the Internet and intended for legitimate purposes. For example, in January 2000, three Randolph High School sophomores allegedly used a keystroke recorder program downloaded from the Internet to note teachers' passwords as they logged onto certain machines in the school's computer network. Armed with a biology teacher's password, obtained when he logged onto a library computer, the three, pretending to be the teacher, found a copy of the biology midterm examination and sold it to some of their classmates.

Keystroke recorder programs allegedly were installed on at least four computers in the school network. Such programs can be used legitimately to back up data to mitigate the effects of hard drive crashes or screen freezes. Parents also can use them to monitor their children's activities on the Internet. The Randolph High students also allegedly loaded another program, called a password buster, on several computers. That software moves progressively through all known words in the dictionary attempting to match a password and gain admittance to the network.

More secretive and complicated techniques also circulate widely in the hacker underground. Thomas Welch, Chief Executive Officer of Secure Data Technologies Corp. of Fairfield, New Jersey, testified how conventions help to spread the word about successful hacking techniques:

> [Hackers] use the same concepts as private business; they have conventions. They have a major convention in Las Vegas every year … had a major convention in New York about three or four years ago. They share their secrets at these conferences and conventions.
> One of the concepts of hacking is information is free and it should be shared, and they do a very good job of sharing their information. Unfortunately, we in the security field don't do the same type of sharing with our own knowledge, and that's one thing we have to learn from the hacker groups themselves.

Edward Skoudis described the challenge of coping with the collegial hacker community:

> What we're seeing today is the rise of … very elite hacker groups. …[I]t's a fairly large number turning out extremely high quality attack software. … [P]oint [the software] to the machine … and it will attack that machine across the Internet. The [hacking] software that's coming out is very well-written, in fact, remarkably free of errors compared to some of the commercial software that's available, and the stuff is available for free across the Internet — point and click with a very simple graphical interface. It's actually quite impressive. And these hacker groups are sort of becoming the Microsofts of the hacker world, turning out their own products, releasing it widely to the world so anyone can download it and use it.

"Sniffers" are programs that unobtrusively monitor network traffic on a computer, picking out whatever type of data they are programmed to intercept, such as any portion containing the word password. When a user logs into an account from a remote location, unless she takes special precautions, her password is sent, unprotected, through perhaps hundreds of computers. Routers are big computers that act as traffic cops, directing the flow of information

traffic from one crowded room to another. A sniffer installed on a router has the potential to acquire thousands of passwords. Although sniffer tools, which “listen” over the Internet to intercept communication, criminally violate federal wiretap law, see 18 *U.S.C.* §2511, such tools have proliferated.

A "Proggy" is a computer program that enables online criminals to steal passwords and credit-card numbers, so that they can use their victims’ online identities to send offensive messages or execute financial transactions. Hackers post proggies around the Internet and trade them like baseball cards. Attacks with proggies have been especially prevalent on America Online, in part because of that ISP’s size. They typically involve "phishing" (*ph* for *f* is a common hacker substitution) for other users’ personal information. For example, a hacker might transmit a message purportedly from the AOL billing department, requesting that a user "validate" his or her password and screen name so that the service can "fix" its records. The hacker might threaten to terminate the user’s account if he does not comply. "Carding," a form of phishing, employs various tricks to obtain a user’s full name and credit card information. Hackers who engage in such activity are called "snerts," an acronym for snot-nosed egotistical rude twits.

In August 1999, the only hacker ever to make the FBI’s Ten Most Wanted List was sentenced to 46 months in prison on federal computer crime and wire fraud charges that included stealing thousands of credit card numbers. A virtual cult figure among the hacking elite, the defendant often did not use high-tech methods to access computer systems. He sometimes gained access to computers by impersonating company employees over the telephone in order to obtain codes and passwords. The defendant is bound by his plea deal to repay the damages he caused to victim businesses with any profits from any future television or book deals.

The court ordered that for three years after his release from prison, the defendant may not touch computer hardware, software, peripherals or modems, and he may not work in the computer business in any capacity. The 35-year-old high school dropout was arrested four times for hacking during the 1980s and previously served a one-year prison term. Prosecutors alleged that while on probation in 1992, the defendant began hacking again. He remained a fugitive until captured in February 1995. Incarcerated since that time, he was released from custody on January 21, 2000 after receiving credit for time served. The sentencing court acknowledged that monitoring the defendant, who once breached the security of government computers and became an underground legend among some young computer enthusiasts, might prove impossible for probation officers.

In a 1998 war game, run by the National Security Agency, it was shown that hackers could disable the U.S. Pacific Command and shut

down the national electrical grid. Hackers have boasted in U.S. Senate testimony that they can bring down the national telephone network. In February 1998, a teenage Israeli hacker, known as "Analyzer," claimed to have high-level access to as many as 400 unclassified systems.

Unless proper defenses are in place, a hacker may “spoof” a domain name system (DNS) server — convincing it, without permission, that he is something or someone that he is not. The Internet uses the DNS to connect numerical Internet protocol (IP) addresses to user friendly Internet names. Once a DNS server has identified the IP address of the site the user seeks, it stores that entry for future reference. If the DNS server is compromised, forged data can be planted. As a consequence, the compromised DNS server now directs the user to a forged IP address substituting for the genuine site name. Users may be directed to a spoofed Web site containing offensive, untrue or damaging content. E-mail can be rerouted to another mail server and, unknown to the sender, never reach the intended recipient. A phony site may collect user names and passwords from unsuspecting users seeking entry authorization. After entering the authorization information, users may be misled with a message saying the site is temporarily unavailable and would never know they had been spoofed. The owner of the fake site then would possess a collection of user names and passwords to use at the real site.

Hackers gain access through a variety of other means. These include scanning, trashing, barrier code hacking (via guessing or "brute force") and remote administration hacking. Mr. Skoudis described the need for proper modem control:

> Oftentimes the easiest way to break into a network is to do a “war dial.” A war dial is a tool that you use to dial a sequential set of telephone numbers … up through thousands and thousands looking for a modem on a network. If you find that modem, then you can use that potentially to get into the network, because oftentimes, individual users will bring in their modem and put it on their desktop so they can access their system at home. Well, it’s also easy for the attackers to get into the network because when these things are set up by individual users, they’re often not protected. So having effective modem policy and conducting periodic scans, to do your own war dial against your … institution, is a very good idea to eliminate these back-door modems.

Mr. Degnan described the need for proper Web site control:

> Everybody has a Web server. The State of New Jersey has a Web site, and everybody else has Web sites; the government is fraught with them. … Now, some [of] those Web sites [are] not authorized, and that is one of the easiest ways to break into a computer

system, through the Web site. So you need to isolate that and put that on a stand-alone computer system with one address ….

Organized crime has joined the act, cashing in on schemes to divert funds through bogus electronic transfers. For example, an "inside/outside" job begins when a prospective victim company hires a computer expert to build a network. For a small fee from a corrupt group, this administrator will deliberately make a “dumb mistake,” leaving an electronic hole through which others can siphon money to private bank accounts.

PASSWORD TIPS

Experts often say that the security of the system is the security of the weakest password. Some of the blame rests on users who pick bad passwords such as someone's name, a birth date or a word from a dictionary. These may be easier to remember, but they also are very easy to break. The following security tips offer protection for passwords.

When creating a password:

- **Don’t** use names or numbers associated with you in any form, i.e. your user name, your spouse’s name, your dog’s name spelled backward, your telephone number transposed, your middle name in French, etc. Hackers are sophisticated enough to make an educated guess.

- **Don’t** use names or dictionary words, including several words strung together, in any language. Sophisticated password cracking programs can discover passwords with effective dictionary or brute force attacks.

- **Do** use upper and lower case letters, as well as punctuation symbols or numbers, for passwords that are several characters long.

- **Do** use different passwords for different accounts and for screen savers and share passwords. An intruder who cracks your password on one network can use it to jump to other networks where you also use it. The same applies to each Web site and Internet business that requires passwords.

Once you have a password:

- **Do** change it frequently, at least every four to six months. If you need to use the same basic word as your password, vary it

with unexpected numbers, symbols or misspellings. Sniffer programs that intercept passwords are quite common, and changing your password offers at least some protection.

- **Don't** e-mail your password to anyone.

- **Don't** tell anyone your password, no matter who asks for it. If someone calls you claiming to need your password, refuse to provide it. Any legitimate technician already will have authorization to enter your system. If, for any reason, you must share your password, change it as soon as possible. Some secrets are too tempting not to use or share.

ENCRYPTION

Encryption is the mathematical encoding of files and data, via software, in such a way that, even if accessed by an intruder, they cannot be read or viewed by anyone other than those with the secret key to decode the message. Original text (known as "plaintext") is transformed into unreadable text (known as "ciphertext"). Although someone may successfully access encrypted data or communications, he may not use them for improper purposes if encryption renders them unintelligible and the intruder cannot break the code. Even relatively sophisticated encryption is readily and inexpensively available to businesses and individuals. For example, Pretty Good Privacy's (PGP) Help Team of volunteers offers freeware encryption software at www.pgpi.com. The program uses a system of complementary public and private keys to encrypt and decrypt e-mail and other electronic files.

Public-key infrastructure (PKI) encryption is a popular method for securing data transmitted online for e-commerce or other purposes. It uses complex mathematical "keys" to encode and decode data. The public key, used to encrypt the message, is one of two keys necessary in a public or asynchronous (asymmetric) cryptographic system. The public key usually is advertised to the rest of the world. The private key, which usually is maintained secretly by its owner, is used to decrypt the message. "Strong" encryption involves programs using larger and, therefore, infinitely less decipherable keys.

In the United States strong encryption has always been available to anyone. Until early this year, the federal government prohibited virtually all export of strong encryption technology. On September 16, 1999, however, the White House agreed to permit U.S. companies to sell even the most powerful data-scrambling technology overseas to private and commercial customers after a one-time technical review of their products. Exporters still have to seek permission to sell encryption technology to a foreign government or military, and no sales can be made to seven nations accused of terrorism: Iran, Iraq, Libya, Syria,

Sudan, North Korea and Cuba. The federal government adopted the new regulations in early 2000.

Federal intelligence and law enforcement agencies contend that organized criminals, terrorists, and hostile governments will elude detection if strong encryption is generally available without permitting government access to users' keys, if necessary. Encryption advocates retort that criminals can be caught by other methods. The issue of government access to encryption keys has become caught up in free speech, privacy and economic debates. Organizations such as Americans for Computer Privacy have opposed federal efforts to control encryption. Some companies maintain that previous federal control over the export of hard-to-break encryption technology crippled exports and impeded the adoption of anti-hacker defenses by U.S. companies and citizens.

For years, the federal government had designated an IBM-developed mathematical algorithm known as data encryption standard (DES), a secret, 64-bit key encryption scheme, to be the allowable format for non-classified information. Critics have long suspected that the government secretly weakened DES to enable surveillance teams to crack messages easily. During a security conference contest in January 1999, a team composed of privacy advocates, the Electronic Frontier Foundation and a group called Distributed.net broke the DES code and cracked a message encoded with it in less than 23 hours. Advanced encryption standard (AES) is a new, tougher algorithm for the latest generation of encryption products.

Sophisticated criminals, including terrorists, have for some time been able to buy or download powerful encryption technology made outside the United States. Now that the White House permits the export of state-of-the-art U.S.-made encryption software, it is urging Congress to give the FBI $80 million over the next four years to develop techniques to break messages scrambled to shield criminal enterprises.

Existing encryption schemes to protect financial transactions, national security information and other significant communications suffer two weaknesses: the numerical-based keys are potentially vulnerable, and they can be intercepted. By contrast, photon-based quantum cryptographic keys, developed by the Department of Energy's Los Alamos National Laboratory, are generated as needed between the sender and receiver via satellite or optical fibers, creating a random string of numbers known only to them. Any attempt to intercept the shared communication or eavesdrop can be detected because of the message's quantum-based nature. Once the sender and receiver share a unique key, they can code, transmit and decode messages securely. The quantum key-distribution system could provide secure satellite communications among cities anywhere in the world.

Meanwhile, as a computer system security device, strong encryption, by itself, is like putting steel security doors on a grass hut. Hackers typically do not break into computer systems by cracking strong encryption defenses. Instead, they use weaknesses in computer system structure or in application software.

CONTROL PROGRAMS AND METHODS

Effective computer security requires cooperation and coordination between government and the private sector. In addition, a national reporting infrastructure and a central response system are required to protect critical computer systems. Network professionals and the agencies and companies for which they work need to take a proactive approach, based on well-defined policies, in order to guard against intrusions effectively. Given sufficient resources and training, units dedicated to controlling computer crime at the state and local levels of government can play an important role in these efforts.

In response to a blitz by hackers against several leading Web sites, President Clinton announced on February 15, 2000 that several companies had agreed to create a mechanism to share cyber-security information. More than 130 companies formed the Partnership for Critical Information Security. It will work with government to develop new ways for business and government to share threat and vulnerability information. The President also authorized funding to create a federal Institute for Information Infrastructure Protection.

U.S. national security agencies are erecting their own specialized intrusion defense systems. After hackers repeatedly accessed vast amounts of sensitive information in Defense Department computers, the Pentagon developed a surveillance system to counter such activity. The system relies on “sniffer” software designed to detect certain sequences of computer commands typically used by hackers to try to sidestep the security features on government computer networks. All communications involving the Pentagon’s main unclassified computer system are now routed through eight large electronic gateways that will be easier to monitor than thousands of “back-door” connection points previously in existence around the world. The system must still contend with “parking tools” installed by the intruders. Such electronic “trap doors” may be used to evade detection devices and to secretly regain access to a system. The Pentagon recently assigned U.S. Space Command the responsibility of coordinating both the defense of military computer networks and attacks on enemy networks.

In September 1999, the Clinton Administration introduced a broad plan to protect the federal government’s non-military computers against intrusion. Intended as a computer security model for the

nation, the proposal includes a Federal Cyber Service Initiative to focus on detecting intruders as they attempt to break into critical systems. The Initiative also would create a Center for Information Technology Excellence to train federal workers to meet the new security challenges. In addition, the Initiative would train a special cadre of students, called a Cyber Corps. In return for college scholarships, students in the Corps would agree to work for a time in computer security after graduation.

The Initiative includes a proposal for a system to alert officials about intrusions involving a small number of very critical computer systems within the federal government. This Federal Intrusion Detection Network (known as FIDNet) would be completely installed by the year 2003.

Under FIDNet, the federal General Services Administration would collect data from civilian agencies, such as the IRS and Department of Health and Human Services, whenever they encounter computer-security problems. FIDNet would forward evidence of criminal activities to the FBI for investigation. The broader presidential plan directed critical industries to create their own cooperative anti-hacker defenses and to forward information about hacker attacks to the federal government.

In October 1999, the banking industry became the first of several industries to create a private computer network to share information anonymously about electronic threats from rogue employees, software viruses and hackers. The Financial Services Information Sharing and Analysis Center, built by the Reston, Virginia-based consulting company, Global Integrity, operates from a secret location. Only licensed banks and other government-regulated financial firms that become subscribers can exchange information or learn details about known security threats. Names and other identifying details are excluded from submissions to ensure anonymity. Although the U.S. Treasury Department helped organize the Center, federal agencies will not eavesdrop on the threat information disclosed by banks, but they will volunteer details about security problems through the FBI’s National Infrastructure Protection Center. These aspects will encourage reporting by financial institutions that otherwise would be concerned about misuse of the information by competitors or reactionary scrutiny by regulators. Center organizers expect 500 to 1,000 financial institutions to join the network by April 2001.

Similar centers are planned to better protect the nation’s most important industries from computer-system intrusion. They include oil, gas, telecommunications, electrical power, transportation, emergency services and water supply.

Civil liberties groups, such as the Washington-based Center for Democracy and Technology (www.cdt.org) have criticized FIDNet as a potential invader of privacy, but there is much support in Congress

for the development of anti-hacker defenses. Opponents, such as the Electronic Frontier Foundation (www.eff.org), claim FIDNet's contribution to needed hacker defenses will be minimal compared to the risk of abuse. Some companies argue that information sharing is unnecessary because, sooner or later, the marketplace will develop strong anti-hacker defenses. They contend that society should emphasize plugging holes in computer security rather than establishing a huge monitoring system.

While the debate over FIDNet and other information sharing systems proceeds, the 35-person, federal Critical Infrastructure Assurance Office (CIAO) continues to coordinate government-wide anti-hacker efforts and to persuade established industries to share information about computer-hacking incidents, technologies and vulnerabilities pursuant to a National Information Systems Protection Program. The CIAO thus far has failed to establish a consensus among federal government agencies, and some high-tech companies have refused to cooperate.

The Federal Government already had become extensively involved in intrusion detection through the inter-agency National Infrastructure Protection Center (NIPC), located at FBI Headquarters. Created in 1998, the NIPC includes personnel from the Defense Department (which has an Intrusion Detection Plan), the intelligence community and other federal agencies, including the President's Commission on Critical Infrastructure Protection. States are represented, and there is an Outreach Program.

The NIPC's efforts to build alliances with its foreign counterparts and affected industries paid off recently with the arrests in March 2000 of two alleged hackers, both 18 years old, in Wales, U.K. The defendants were charged with breaking into Internet sites, stealing information on more than 26,000 credit card accounts, and posting some of it on the Web. Over several months, the defendants allegedly intruded on nine e-commerce Web sites located in the United States, Canada, Thailand, Japan and the United Kingdom. The FBI, local police in Wales, Royal Canadian Mounted Police and Internet security consultants, assisted by the international banking and credit card industry, investigated the case.

The NIPC has a broader focus than the FBI's Computer Investigations and Infrastructure Threat Assessment Center (CITAC). The NIPC gathers intelligence from private industry, domestic and foreign governments and other sources. It responds to reports of computer intrusion and sponsors educational efforts within industry and law enforcement. The NIPC investigates cases involving teenage hackers, organized crime groups, terrorist organizations and economic espionage.

A recent offshoot of the NIPC, InfraGard, involves businesses and schools around the nation in protecting information systems. Chapters throughout the country, including one launched in New Jersey in November 1999, receive funding and administrative support from the FBI. Membership is free and includes encrypted access to a secure Web site through which members can exchange experiences and solutions, anonymously if desired. In return for agreeing to report actual or attempted disruptions of their computer networks, members receive non-classified information on investigations that is not available to the public, early alerts on threats, and training on vulnerabilities from government and academic experts on security, including some from Princeton University. The New Jersey chapter was organized by the FBI's Newark division and is one of 56 such partnerships around the country. It started with two dozen companies, including PSE&G, IBM and TD Waterhouse Securities. The New Jersey Division of State Police participates in the InfraGard program.

The FBI's National Computer Crime Squad (NCCS) is located within the Washington Metropolitan Field Office. It has national jurisdiction and investigates violations of the federal Computer Fraud and Abuse Act of 1986, which includes intrusions into government, financial, most medical, and "federal interest" computers. A commercial computer victimized by an intrusion coming from another state is a federal interest computer.

The Computer Emergency Response Team (CERT®) Coordination Center (www.cert.org) is part of the Networked Systems Survivability Program in the Software Engineering Institute, a federally funded research and development center at Carnegie-Mellon University in Pittsburgh. Founded in 1988, the Coordination Center serves as a public sector information sharing and analysis center (ISAC). It collects and responds to reports of computer security problems, including password-based attacks. CERT is available on a 24-hour-a-day, seven-day-a-week basis and receives far more requests for help than it can handle. As a result, it deals with incidents on a triage basis, tackling the most far-reaching crises first. One incident reported to CERT in July 1998 involved an intruder with a list of 186,000 passwords collected from businesses and universities all over the world.

The Forum of Incident Response and Security Teams (FIRST) (www.first.org), was established as a worldwide coalition of about 70 government, commercial and academic organizations cooperating and coordinating to prevent and rapidly react to security-related incidents affecting computer systems and networks. It promotes information sharing among its members and the general public. Eleven initial members founded FIRST in 1990.

Computer security consulting is a rapid-growth industry. For example, ICSA.net, Inc. (formerly the International Computer Security Association, Inc.) assesses security threats and evaluates anti-virus

software for large corporations. The Big Five accounting firms also have consulting groups to help clients cope with penetration of their computer systems. The International Association of Computer Investigation Specialists in Portland, Oregon (www.cops.org) provides training to law enforcement officials. InfoWar.Com (www.infowar.com) sells computer hardware, software and books relating to computer security. It also provides free news and information regarding high-tech security issues, including a free newsletter.

Tracing those who use the Internet, whether by sending e-mail or otherwise, can be easy or impossible, depending on the sophistication of the user. Every Internet user leaves behind “digital footprints” that investigators may trace, similar to the way they use telephone records. E-mail messages contain “header” information that leaves an audit trail of their journey through cyberspace. Online accounts that people use to surf the Web or send e-mail are assigned a unique stamp, an Internet protocol address, that helps direct the exchange of data between a Web site and its visitors. The IP addresses leave digital footprints that may lead to cyber-hooligans, even if they attempt to conceal their identities with pseudonyms, fake e-mail addresses and stolen ISP accounts. Investigators also may trace intruders with serial numbers embedded in documents written with popular word processing programs. Also, ISPs are growing more willing to provide timely release of user logs to investigators in response to warrants or subpoenas.

"Ethical hacking" (sometimes called "white hat hacking," “tiger team testing,” “penetration testing” or “intrusion testing”) pits inside or outside experts against a computer system’s security defenses in order to expose weaknesses and inadequacies. The security experts "beat on" security products looking for flaws. They also analyze the latest hacker tools.

LOpht (pronounced "loft"), based in South End loft space in Boston, is a several-person hacker think tank that claims to have a public-service mission to publicize computer system flaws in order to strengthen security. When they find vulnerabilities in supposedly secure systems, they publish their findings on the Web in the hope that the companies that created the vulnerable software will fix the problems (sometimes called “exploits”) for their customers. LOpht’s members identify themselves only by their hacker nicknames, such as Mudge, Space Rogue, Kingpin, Weld Pond and Brian Oblivion. Several were called to testify before the U.S. Senate Committee on Governmental Affairs in May 1998.

Although many corporations have implemented significant measures to protect their computer systems from unauthorized access, many others have done little, thus placing their systems in extreme jeopardy. A good program to tighten computer security carefully assesses needs and develops a plan. With proper hardware and software

in place, the company should thoroughly train employees and monitor the system that is installed. The company should respond instantly to security threats and involve law enforcement where appropriate.

After proper safeguards have been installed to keep down the cost, companies may purchase insurance to mitigate the consequences of unauthorized access to a computer system. At least one joint venture now offers up to $50 million of insurance coverage against the effects of external or internal intrusions.

Despite all the efforts within the public and private sectors to convince businesses to report unauthorized intrusions, their reluctance to do so remains a significant problem. A company often fears, with some justification, that if it informs the government of a hacker attack, its business reputation and bottom line will suffer as the security breach or the information itself is leaked or presented in court. A survey by the U.S. military indicated that 90 percent of computer offenses are not reported. A survey of businesses in New Zealand concluded that 70 percent would rather have suspected activity investigated privately than involve the police. However, the willingness to report may be improving. A striking finding of the Computer Security Institute's "1999 Computer Crime and Security Survey" was the dramatic increase in the number of respondents reporting serious incidents to law enforcement: 32 percent compared to only 17 percent in the three prior years of the survey.

Most businesses are afraid to complain to law enforcement for fear of exposing security vulnerability. Companies want to avoid public relations disasters adversely impacting reputation. Despite the government's ability to gather evidence through compulsory process not available to the private sector, companies are concerned that their ability to gather the information they need to stop the intrusions and to find the perpetrators may be restricted once the government becomes involved. Corporations also fear that making it known to law enforcement that intruders penetrated their defenses may invite government regulation. They would rather institute their own system to ward off attacks than comply with government-dictated controls.

For there to be an effective partnership between law enforcement and the business community, the latter must have confidence that any security breaches referred to law enforcement will be handled as swiftly, competently and confidentially as possible. The likelihood that corporate victims will report intrusions to law enforcement will increase if (1) law enforcement's technical proficiency and reaction time improves, and (2) the investigation and discovery phases of cases adequately preserve confidentiality. Law enforcement expertise and resources must be available to handle a high volume of routine cases as well as high profile matters, such as the notorious Melissa computer virus case, which led to guilty pleas by

the defendant in state and federal courts in New Jersey in December 1999.

In March of 1999, a new breed of computer virus was launched, called the "Melissa" virus. Unlike previous computer viruses, the Melissa virus spread through e-mail systems and multiplied at an exponential rate crippling tens of thousands of e-mail systems worldwide, including systems belonging to governments, the military, academia and business. Within a few hours of its launch on March 26, 1999, computer systems were impacted from the United States to Japan. While the virus was isolated within a few hours, the incredible rate at which it reproduced meant that there was very little that could be done to stop it.

Almost immediately, experts from throughout the United States and Europe began looking for the person responsible for the creation and spread of the Melissa virus, one of the most disruptive computer viruses in the short history of the Internet. Over the weekend of March 27 and 28, 1999, federal law enforcement agencies and private computer sleuths scoured the Internet looking for clues about the source of the virus.

On March 29, 1999, a representative from the world’s largest Internet service provider, America Online, provided the New Jersey Division of Criminal Justice (DCJ) with information identifying New Jersey as a possible source of the Melissa virus. Within a few hours of that telephone call a significant array of state computer investigative resources was assembled to track down the leads provided. DCJ, which had a specially trained prosecutor and three high-tech crime investigators, teamed with the specialized computer crime unit in the New Jersey State Police to form a task force to find the virus’ creator. On March 30, 1999, America Online supplied the team with the information that it had developed. Working round the clock, the task force was able to identify the source of the virus, its creator and his whereabouts by April 1, 1999. The task force was expanded to include the Newark Field Office of the FBI and the U.S. Attorney’s Office for the District of New Jersey. It apprehended the Melissa virus’ creator in the evening of April 1, 1999. In cooperation with the U.S. Attorney’s Office, the case was prosecuted in federal and state courts. Following guilty pleas by the defendant, sentencing was scheduled for August 2000.

The “Melissa” investigation was a landmark case, not only because of the devastating effects of the virus and the unusually quick determination of its source, but also because it was the first such case to showcase state technological expertise. A lasting legacy of the investigation is the Statewide Computer Crime Task Force, which includes members from the divisions of Criminal Justice and State Police and investigative personnel from county and municipal law enforcement agencies.

Matters that federal enforcers reject for prosecution — due to the application of a high threshold of monetary damages, for example — should be candidates for state enforcement action. The U.S. Justice Department's David Goldstone testified about the need for effective state-level enforcement:

> As I said, the leading cause of attacks in the private sector is disgruntled employees. Those attacks will tend to be effectively local crimes. … [T]hose kinds of crimes may be crimes that state law enforcement may be in the best position to investigate and prosecute.
>
> In addition to that, there's another class of crimes … relating to juveniles, where juveniles are given often free rein by parents and even teachers to spend a lot of time unsupervised on a computer. With the … easy availability of hacker tools out there, it is very easy for juveniles, even if they're not computer whizzes themselves, to wreak havoc and to get themselves into an awful lot of trouble. … [I]n most cases involving juveniles, we, the Federal Government, feel the appropriate response is to refer the matter to the state because … New Jersey has good provision for these services that supervise juveniles.
>
> Nevertheless, our experience from the Department of Justice is that in many states when the Division of Youth and Family Services is confronted with a juvenile who's a hacker, by comparison to the other juveniles under their supervision, these malefactors look comparatively good. They're not crack dealers. They're not violent. And with limited resources, [these juveniles] will not get any kind of supervision, which is, of course, what got them into trouble in the first place.

Seeking civil remedies is another approach available to corporate victims or their insurers. Mr. Goldstone testified about the frequent ineffectiveness of this approach:

> Civil penalties, of course, have an important role to play. I think it is important also to recognize the limitation of the civil means. First of all, investigating computer crime cases is very difficult. Hackers give the appearance often of anonymity, and it is very hard to investigate the cases. Now, law enforcement, through its subpoena power and its ability to get court orders for information from various Internet providers, as well as search warrants as need be, can often be much more effective in investigating crime than a civil party … by itself. Second, the amount of damage that a hacker can do to a victim often can be in the tens of millions of dollars. Most hackers will be judgment proof, and a civil remedy will not be a substantial deterrence.

INTERNET FRAUD

COMMON SCAMS SPREAD FAR AND FAST ONLINE

John Kenneth Galbraith once observed that “the man who is admired for the ingenuity of his larceny is almost always rediscovering some earlier form of fraud.” Nearly all of the fraudulent schemes found on World Wide Web sites and in e-mail are simply revised versions of tried and true telemarketing or mail frauds that have been fooling the unwary and the gullible greedy for centuries. The schemes involve high-pressure sales tactics, refusal to provide written information, and unrealistic claims of potential profits or earnings. Perpetrators take advantage of the culture of benevolence and trust on the Internet, as well as the multitude of opportunities presented by instant access to millions of potential victims. Thus, the need to be vigilant and report wrongdoing is greater than ever.

The National Consumers League (NCL) operates the National Fraud Information Center, which estimates that there are 14,000 illegal telemarketing operations bilking U.S. citizens of at least $40 billion annually. Meanwhile, the proportion of fraudulent activity attributable to online schemes is growing almost exponentially. For example, Internet Fraud Watch (IFW), also operated by the NCL, reported that the number of Internet fraud complaints it received rose recently by 600 percent, from 1280 in 1997 to 7,439 in 1998. In the first six months of 1999, IFW received over 8,000 complaints.

The Internet has created a whole new set of opportunities for defrauders and problems for law enforcement. It is a powerful tool helping swindlers overcome their two greatest challenges: identifying victims and contacting victims. What is striking is the size of the potential market and the relative ease, low cost and speed with which a scam can flourish over the Internet. Victims may never have the opportunity to see or even speak to the defrauder.

Eileen Harrington, Associate Director for Marketing Practices of the Federal Trade Commission’s Bureau of Consumer Protection, testified that online defrauders benefit from “the very characteristics that make e-commerce grow”: anonymity, the distance between the buyer and the seller, and the instantaneous nature of the transactions. She added, “Fraudulent operators on the Internet take advantage of the fact that this marketplace is still a confusing one to consumers.” Ms. Harrington emphasized the confounding speed of online scams:

> I think that with the Internet as the medium, everything happens more quickly. The business sets up more quickly. They change identities more quickly. I mean, you can throw up a new Web site in an hour. It just has moved things to kind of a warp speed. So you find that the life-span of one of these frauds is much shorter than might have been the case where the frauds turned out to rent office space, get phone lines, [and] do all of those sorts of things. We find more and more that these scams are operating out of homes.

Noting that fraud over the Internet requires access to some form of payment system, just as every other kind of fraud does, Ms. Harrington urged consumers to pay for their online purchases by credit card. She explained that "consumers have important federal rights that protect them from being held liable for unauthorized and fraudulent transactions if they pay by credit card."

Susan Grant, Vice President for Public Policy of the National Consumers League (NCL) and Director of the NCL's National Fraud Information Center and Internet Fraud Watch programs, testified as to why consumers must take extra care in cyberspace:

> I think that people sometimes get so excited about the novelty of the Internet that they lose sight of the same common sense that they would use if somebody knocked on their door in the middle of the night offering them something, and it was a stranger, or if they got a telephone call out of the blue from somebody that they didn't know.
>
> There's a lot of talk about community on the Internet as though it's one big happy place with everybody dedicated to the pursuit of knowledge and sharing information with each other, but in fact, just like any community, there are bad guys lurking in the alleyways. People need to be cautious. It's no reason not to use the Internet.
>
> And actually, I think it's ironic that, for instance, we see a decreasing amount of credit card use for payment compared to things like checks and money orders, and yet the credit card is the safest way to pay because of your legal dispute rights.
>
> I think that people may be so worried about giving their credit card information on the Net, even though with the encryption programs that are in place, it's really, from what we can see, relatively safe. And they're not sufficiently worried about who it is that they're doing business with at the other end.

Online auctions alone are expanding e-commerce rapidly. Gomez Advisors estimates that in 1999 online auctions connected 7.4 million buyers and sellers transferring goods worth $4.5 billion. The

independent firm, which rates Web sites for consumers, expects online auction sales volume to exceed $9 billion in 2000. According to IFW, online auction complaints led all others with 68 percent of the Internet-related fraud complaints it received in 1998. Auctions also were first in 1997 with 26 percent. During the first six months of 1999, IFW received 5,287 auction complaints, surpassing the 5,236 it received in all of 1998.

IFW reported that 93 percent of payments in response to fraudulent Internet schemes were made “offline” by check or money order sent to the defrauding company. By and large, consumers failed to follow the safest course, which is to pay by credit card so that the charges can be disputed if there is a problem. Giving cash, a check or, worse, a bank-account number can make it impossible to get a refund from online vendors. Since online auction sellers often lack proper equipment to take credit card payments, IFW recommends that buyers use escrow services, which hold payment from the buyer and only pass the money along to the seller after verification that the goods or services were satisfactory. Insurance is another safeguard that sometimes proves beneficial.

Once online, consumers are bombarded with unsolicited commercial e-mail (known as "spam") advertising everything from legitimate services to fraudulent investment schemes. Millions of messages can be sent out in a very short period. Although schemers can easily purchase e-mail address lists from companies that do business online, they also can use “harvester” software to conduct worldwide searches of Usenet newsgroups, Internet directories and chat rooms in a very short amount of time. In this way, they can collect thousands of e-mail addresses for individuals likely to be vulnerable to certain types of schemes. Others pirate names and e-mail addresses from membership directories of Internet service providers. Spammers also use software that generates e-mail addresses at random. Thus, people can get spam even if they have never made online purchases or entered chat rooms.

Web sites abound offering both legitimate and fraudulent products and services. Since buying online essentially is buying sight unseen, the honesty of the seller is paramount. This is particularly important in the booming online auction business.

The rapid growth of e-commerce has significantly transformed the U.S. securities industry. In 1998, about 14 percent of all securities trades were conducted online compared with virtually no such transactions in 1995. However, this understates the impact on the small investor because approximately 37 percent of all individual trades are now online, up from 17 percent in 1997. Three million people had online trading accounts in March 1999, a number expected to reach 14 million by 2001.

Online investing is generally a positive development, giving investors unprecedented access to company and investment information and individual trading services. As in other areas, however, the Internet has provided dishonest operators with an efficient medium to defraud investors. The U.S. Securities and Exchange Commission reported a 330 percent increase in complaints regarding online investments in 1998. Its Office of Internet Enforcement receives between 200 and 300 complaints every day, of which 70 percent allege Internet securities fraud. Many investors have not developed proper skepticism about the quality some of the information they encounter online.

Robust education is even more important for cyberspace consumers than it is for those buying in other marketplaces. The average consumer has difficulty distinguishing between legitimate Web sites and those that are scams. Anyone can put up on the Web a reputable looking site. Criminals forge header information to mask their identities and locations. Some cyber-crooks use "throw away" accounts (easily created and discarded free accounts) and forged headers to make it appear that testimonial e-mail and postings come from many different people rather than from the crook himself.

COMMON FRAUDULENT SCHEMES

Common fraudulent schemes found on the Internet and elsewhere include:

- **Online Auction Frauds**. Sellers may not deliver items, or their value may be inflated. Sometimes shills drive up the bids. In early 1998, the National Consumers League placed auction frauds at the top of its list of Internet scams and cautioned consumers to investigate any auction site before placing a bid. The FTC, which received approximately 10,000 complaints about Internet auction fraud in 1999, has issued similar warnings. Online auction buyers can guard against fraud by placing payments in escrow accounts rather than sending them immediately to the sellers. For details, see i-Escrow® at www.iescrow.com. Alternatively, using a charge card makes it easier to obtain a refund. Also, some auction sites, such as the popular eBay, sell fraud insurance. Ebay’s Fraud Prevention Department takes complaints from its Community Watch program and proactively monitors and suspends accounts. Transgressors are referred to government authorities.

- **General Merchandise Rip-offs**. These involve sales of everything from T-shirts to toys, calendars to collectibles. The goods are never delivered, or they are not as advertised.

- **Bogus Sales of Hardware or Software**. Purchased computer products may never be delivered, or they may not be as represented.

- **Shady Sales of Internet Services**. There may be charges for services that were touted as free, failure to deliver on promised services and false representations of services.

- **Work-at-Home Schemes**. Two popular versions offer the chance to earn money by stuffing envelopes or assembling crafts at home. However, nobody is paid for stuffing envelopes or craft assembly since promoters, claiming the work does not meet their "quality standards," usually refuse to buy the finished product.

- **Business Opportunity Scams**. These promise significant income for a small investment of time and money in a business — often a franchise. Some are actually old-fashioned pyramid schemes camouflaged to look like something else.

- **Chain Letters, Pyramid Schemes and Ponzi Schemes**. Any profits are made from recruiting others, not from sales of goods or services to end-users.

- **Guaranteed Loans or Credit on Easy Terms**. Some schemes offer home equity loans, even for those who lack equity in their homes. Others offer guaranteed, unsecured credit cards, regardless of the applicant's credit history. The "loans" turn out to be lists of lending institutions, and the credit cards never arrive.

- **Credit Repair Frauds**. Sometimes called "file segregation," these schemes are pitched over the Internet and e-mail to consumers with poor credit histories. They lure consumers into breaking the law by creating fake credit histories with substitutes for their genuine social security numbers. Consumers pay fees as high as hundreds of dollars to the so-called credit repair companies. They are then instructed to apply to the IRS for a taxpayer or employee identification number, which is then substituted for their nine-digit social security number. Thus, the credit repair scams actually turn gullible consumers into criminals by advising them to use false identification numbers to apply for credit. Scam operators also offer to clean up credit histories for exorbitant prices. The reality is that consumers can obtain information about their credit history and correct inaccuracies for free. If a credit report is accurate, it cannot be "fixed." By federal law, credit repair organizations must give customers a copy of the pamphlet "Consumer Credit

File Rights Under State and Federal Law" before a contract is signed.

- **Advanced Fee Loans.** These scams prey upon people's desperation to obtain loans. Operators claim that for a fee they can find loans despite the victim's poor credit history. They also claim to be able to provide favorable interest rates or other advantageous terms. Upon paying the advance fee, however, the victim never hears from the scammer again.

- **Employment Offers and Easy Money Schemes**. Phony offers such as "Learn How to Make $4,000 in one day," or "Make unlimited profits exchanging money on world currency markets," appeal to the desire to get rich quickly.

- **Bulk E-Mail Scams**. Victims are sold lists of e-mail addresses and software with the claim that this will enable them to make money by sending their own solicitations via bulk e-mail. However, the lists are of poor quality; sending bulk e-mail violates the terms of service of most Internet service providers (ISPs); virtually no legitimate businesses engage in bulk e-mailings; and several states have laws regulating the sending of bulk e-mail.

- **Health and Diet Scams**. These bogus cure-alls are just electronic snake oil.

- **Get Something Free Scams**. Consumers pay membership fees to "qualify" to obtain free items, such as computers or long-distance phone cards. After paying the fees, they learn that they do not qualify until they recruit other "members."

- **Fraudulent Stock Offerings and Market Manipulation**. In investment fraud, perpetrators (1) create a classy-looking but phony Web page, complete with official-looking emblems, to lure investors; (2) create enthusiastic endorsements from non-existent customers; (3) send spam to potential investors with a hyperlink to the phony Web site; and (4) create phony online "buzz" about the investment in bulletin boards linked to the Web page, discussion forums, chat rooms, and sham or bribed newsletters. In market manipulation "pump and dump" schemes, individuals who own a company's securities spread positive but false information about the company to increase investor interest and drive up the price of the securities. The individuals then sell their securities at a quick profit, while later investors face large losses when the price of the inflated securities declines. One new fraud involves impersonating legitimate brokerage-firm Web sites. Investors believe they are sending money to the broker when, in fact,

the address is a post-office box. When authorities detect them, the perpetrators merely shut down the Web site and impersonate the same or another brokerage firm using a different Web address and another post office box.

- **Stock Day-Trading Abuses**. Stock day trading sometimes involves false advertising or failure to ensure that people have enough money to trade. Ordinary people can gamble on short-term changes in stock prices from firms' trading floors or from home computers equipped with special software. It is very easy for day traders to make mistakes and lose a lot of money, even though they are not defrauded. With huge returns commonplace in the stock market, many people are no longer investing. They are gambling, which makes them more vulnerable to a con game.

- **Cable Descrambler Kits**. For a small initial investment one can buy a kit enabling the receipt of cable television without paying the subscription fees. However, the kits usually do not work, and stealing cable service is illegal.

- **Vacation Promotions (Prizes, Certificates, Clubs, Etc.)**. E-mail informs consumers that they have been selected to receive "luxury" vacations at bargain-basement prices. However, the accommodations are not deluxe and upgrades are expensive. If the seller can delay the travel for 30 to 60 days, it is harder for a buyer to get a credit-card refund. Consumers need to find out if the seller is a travel agent belonging to the American Society of Travel Agents, whose members subscribe to an ethics code and pledge to help resolve complaints. Also, the U.S. Tour Operators Association and the National Tour Association have a restitution fund to protect travelers against company bankruptcies.

- **Fake Scholarship Search Services**. Consumers pay a fee for guaranteed assistance and merely receive a list of financial aid offices or nothing at all.

- **Page-Jacking**. As many as 25 million of the roughly one billion pages on the World Wide Web have been "page-jacked." Perpetrators prepare a page that impersonates an innocent commercial or informational Web site and resubmit it to search engines with a false address. When Web users search for the original site, the sham site opens, often with pornographic material. The page-jackers make money by selling ads, showing clients that they receive a large number of page hits. Of course, the hits come from unwilling users. Users attempting to back up the Web browser or shut it down are merely connected to more pornographic sites. Legitimate site owners

have to ask search engines to remove access to the phony sites, a process that may not occur expeditiously enough to forestall significant losses of profit and reputation.

- **Sham Sweepstakes Prizes**. The perpetrators demand payments before authorizing the release of prizes. Of course, the prizes never arrive.

- **Sound-Alike Charities**. Schemers masquerade as legitimate charities to lure contributions from unsuspecting donors.

- **West African (Nigerian) Oil Profits Deposit Swindles**. Phony "civil servants" ask U.S. citizens for their bank account numbers so that they can assist in investing millions in oil revenues in return for a percentage of the profits. The scheme dupes American investors out of $100 million a year, according to the U.S. Postal Inspection Service. The Service received 108,000 complaints nationally between 1997 and 1998.

- **Bogus Banks and Bank Instruments**. Sham offshore banks, operating online, solicit deposits with offers of huge interest. They claim they can offer such interest because of low overhead. They also claim they can protect customers from government prying.

- **Fraudulent Offshore Trusts**. These are marketed over the Internet as a means to evade taxation.

- **Affinity Frauds**. They target certain religious or ethnic groups.

- **Cyber-Smears**. Perpetrators post false information or fake press releases about companies on the Internet.

CONTROL ORGANIZATIONS AND PROGRAMS

A number of conditions have hampered effective control of online fraud. It is difficult to find reliable statistics on the extent of the problem. Bulwark investigative agencies have only recently joined in the fight against online fraud. Coordination among those agencies is just getting started. Creation of a national strategic plan for the control of such fraud remains in its early stages.

A national education campaign, called "kNOw Fraud™," was launched in November 1999 to warn the public about telemarketing fraud. More than 120 million over-sized postcards listing fraud-prevention tips and contact numbers were mailed to U.S. households. A Web site was established at www.consumer.gov/knowfraud/index.html to explain the

program and provide prevention tips. Complainants may contact the program's toll-free hotline at 1-877-987-3728. Public libraries received 16,000 informational videos. Coordinating the campaign are the U.S. Postal Inspection Service, the Federal Trade Commission, the Federal Bureau of Investigation, the Department of Justice, the Securities and Exchange Commission, the National Association of Attorneys General, the American Association of Retired Persons and the Council of Better Business Bureaus Foundation. Many of kNOw Fraud's awareness tips also will help people to avoid becoming victims of online fraud.

FEDERAL TRADE COMMISSION (FTC)

The FTC has interpreted its enabling legislation as permitting it to regulate e-commerce. It has assumed that its regulations concerning such things as fair marketing practices and mandatory disclosures apply to the Internet. Eileen Harrington, the FTC's Associate Director for Marketing Practices, testified that the agency brought its first enforcement action against a fraudulent operator using the Internet in 1994. By the end of 1999, the FTC had brought 107 such actions against 315 defendants. In February 2000, it published a report, entitled *Going, Going, Gone*, highlighting its efforts to counter Internet auction fraud (see www.ftc.gov/bcp/reports/int-auction.pdf).

The FTC (www.ftc.gov) accepts reports of fraud at its Consumer Response Center over a toll-free Consumer Help Line, 1—877-FTC-HELP (382-4357). Many involve fraud over the Internet. In a joint project with the National Association of Attorneys General (NAAG), the Council of Better Business Bureaus, the U.S. Postal Inspection Service, and Canadian partners, Canshare and Phonebusters, the complaints are entered into a database called Consumer Sentinel. Over 1,000 law enforcement personnel connected to the system via desktop terminals search for repetitive schemes and offenders. Help Line counselors also provide information to the callers. As of June 2000, the database, maintained by the FTC and available to more than 240 law enforcement agencies in the United States and Canada, contained in excess of 250,000 consumer fraud complaints filed with federal, state and local law enforcement agencies and private organizations.

Ms. Harrington testified, "[O]ne of the great benefits of the Internet for law enforcement is that we are more able than we have been with any other medium to see what is going on as it happens and to use the technology to fight the fraud." At its Web page, the FTC operates an online, real-time complaint form. When consumers fill it out, their complaints go directly into the Consumer Sentinel database.

In addition, the FTC pioneered periodic, concentrated, daylong "Surf Days," searching the Internet for targeted fraudulent schemes in partnership with state and local agencies throughout the country. New

Jersey's Division of Consumer Affairs participates in these periodic nationwide enforcement "sweeps." Past targets have included bogus "lotions and potions" health claims, pyramid schemes and credit repair frauds. Scamming Web sites that have blocking programs to screen out anyone using a government computer are accessed by investigators from their home computers.

In February 2000, with the help of agencies in 28 countries, the FTC, assisted by the U.S. Securities and Exchange Commission and the U.S. Postal Inspection Service, targeted more than 1,600 suspect Web sites throughout the world. Law enforcement officers from other federal agencies and 45 states, including New Jersey, participated in the FTC's 21st international sweep of companies touting get-rich-quick schemes over the Internet. The site operators were warned that failure to cease operations or change their claims would lead to enforcement action.

The FTC has a list called the "Dirty Dozen: 12 Scams Most Likely to Arrive Via Bulk E-Mail." Individuals can forward their scam spam (unsolicited commercial e-mail, or UCE) to a special FTC e-mail address uce@ftc.gov. The FTC receives more than 1,000 such messages a day. It also issued a brochure about UCE entitled "Trouble @ the In-Box." In 1998, the FTC published a booklet called "Advertising & Marketing on the Internet: Rules of the Road."

Ms. Harrington testified that the FTC uses the Internet for consumer education. Mimicking fraudulent offers with portions of actual scam pages, FTC staff creates "teaser" Web sites that "look just like what the scam guys do," according to Ms. Harrington. If consumers respond, they view a notice that begins as follows:

> If you answered an ad like this, you could get scammed. We're the Federal Trade Commission. Here are some things that you need to watch out for if you're looking for a home-based business opportunity on the Internet.

The site then directs the surfer to a series of links where consumers can learn how to protect themselves from fraud on the Internet.

On February 2, 1999, the FTC and the attorneys general of several states announced a crackdown on credit repair fraud. In 1997, the FTC joined attorneys general in 12 states in Operation Trip-Up, an effort to curtail travel-scam artists. Various operators were forced to stop offending activities and, in some cases, to repay consumers.

INTERNET FRAUD COMPLAINT CENTER

In 1999, the Federal Bureau of Investigation (FBI) launched the Internet Fraud Complaint Center (IFCC) in Morgantown, West Virginia.

It may be reached through the FBI's Web site or www.ifccfbi.gov. Co-sponsored with the National White Collar Crime Center, the IFCC collects computer crime complaints from the public at its Web site. It also serves as a clearinghouse of online fraud complaints collected from a variety of organizations. Approximately 80 percent of the complaints received do not meet the FBI's threshold guidelines for initiating an investigation. These are forwarded to state and local law enforcement agencies. The National White Collar Crime Center, which receives some project funding from the U.S. Department of Justice, provides analytical support and training to the local and state agencies. It is developing a curriculum for Internet fraud investigations.

The Complaint Center's 150 personnel will develop a national Internet fraud strategy, identify and track fraud, analyze crime trends, triage complaints, develop investigative packets, and forward information to the appropriate agencies. When a fraud has been referred to a particular agency, similar complaints will be referred to the same place. Within the FBI, a group of senior intelligence research specialists conducts Internet fraud investigations.

INTERNET FRAUD COUNCIL

Established in early 1999, the Internet Fraud Council (IFC) (www.internetfraudcouncil.org) is a nonprofit organization of corporations, trade associations and academic institutions working with government and the media on preventing, interdicting and prosecuting fraud committed over the Internet. Based in Richmond, Virginia, the IFC is creating a clearinghouse of information regarding the variety of economic crime perpetrated on the Internet. It is studying and quantifying incidents of Internet fraud and disseminating the information to its members and law enforcement agencies. The IFC plans to develop tools and best practices that can be used by its members to alleviate the threat of cyber-crime to their respective organizations.

Three privately funded anti-fraud groups support the IFC. They are the National Fraud Center (a fraud and risk management consulting firm established in 1982), the National White Collar Crime Center, and the National Coalition for the Prevention of Economic Crime (NCPEC – a non-profit research organization). The IFC, which is a division of NCPEC, provides training to counter Internet fraud and forecasts fraudulent activity. It gathers statistics and identifies trends in online fraud.

The Council also has created a set of standards for companies doing business on the Internet. It offers a fraud-free "seal of approval" for such businesses.

INTERNET FRAUD WATCH

The National Fraud Information Center (NFIC) was established in 1992 to combat telemarketing fraud. In 1996, the Internet Fraud Watch (IFW) was created to operate in tandem with the NFIC, expanding the scope of fraud-fighting efforts to scams in cyberspace. Both are programs of the nonprofit National Consumers League (NCL), which was founded in 1899. The NCL also has an Elder Fraud Project. The NFIC/IFW toll-free hotline is 1-800-876-7060 (Web site: www.fraud.org). Trained counselors help consumers identify the danger signs of fraud.

The Alliance Against Fraud in Telemarketing, a coalition of private sector, government and nonprofit groups coordinated by the NCL, promotes public awareness about telemarketing and Internet fraud. Susan Grant, the Director of NFIC and IFW, testified that New Jersey's Division of Consumer Affairs "is a long time member of the Alliance."

NFIC/IFW is the primary data source for the Federal Trade Commission/National Association of Attorneys General National Fraud Database (Consumer Sentinel), which, in turn makes information about frauds available to law enforcement in the U.S. and Canada on a 24-hour basis. NFIC/IFW also relays complaints to law enforcement, including those filed by consumers using online fraud reporting forms available through the NFIC.

BBBONLINE®

Established in April 1997, BBBOnLine, Inc. is a wholly owned subsidiary of the Council of Better Business Bureaus, Inc. (CBBB). The BBBs contribute complaints about online fraud to the FTC's Consumer Sentinel.

The BBBOnLine Reliability program was designed to help build confidence in the electronic marketplace. Since its creation in April 1997, more than 2,600 companies have applied for BBBOnLine and in excess of 2,300 have been accepted. Of these, more than 2,000 are current, active participants. To be accepted into the program, online businesses must comply with the following requirements:

- Own an operational Web site;
- Provide the BBB with information regarding company ownership and management and the street address and telephone number at which they do business, which will be verified by the BBB in a visit to the company's physical premises;
- Be in business a minimum of one year;
- Have a satisfactory complaint handling record with the BBB;
- Agree to participate in the BBB's advertising self-regulation program and correct or withdraw online advertising when

challenged by the BBB and found not to be substantiated or not in compliance with the BBB's children's advertising guidelines;
- Respond promptly to all consumer complaints; and
- Agree to arbitration, at the consumer's request, for unresolved disputes involving consumer products or services advertised or promoted online.

Approved participants may place the BBBOnLine seal of approval on their Web sites. Each seal links to the BBBOnLine database so a consumer can click on the seal and confirm instantly that the seal belongs to a valid BBBOnLine participant. Online shoppers can access a BBBOnLine profile on the participant. Those seeking reliable businesses of a particular type can search BBBOnLine Reliability at www.bbbonline.org/businesses/reliability/index.html.

BBBOnLine's Web site, www.bbbonline.org, links to many BBB tips for avoiding scams found on the Internet. It also links to other BBB services on the Web, such as online complaint filing, business and charity report lookups and online safe shopping tips.

Russell Bodoff, BBBOnline's Senior Vice President and Chief Operating Officer, testified that most of the problems his organization encounters in e-commerce involve misleading advertising rather than fraud. He added:

> What's interesting when we go back to the companies though, we get almost a hundred percent compliance in making changes to the Web site. So it makes us feel that what we really have – I think it's an opportunity to work together through our local Better Business Bureau and the law enforcement organizations in any given state – is an education process, and reaching out to as many businesses as possible, because we're finding the problem with smaller companies, and that's the excitement of the Internet. … That is, the small business [that] never before could afford to advertise in anything more than a local penny saver, now, through some creativity, can put up a Web site that can make [it] look as good as Fortune 500 companies and can reach [its] audience, but with a lack of sophistication.
>
> So business education I think is going to be extremely critical. It's going to help cut down problems in the future where consumers are going to be misled, not deliberately, but because the company is just not comfortable. Because how many times do we see on the Internet … companies' claims of "world's largest selection" or "world's lowest prices." Well, in off-line media, the company is expected to have substantiation for any of that claim. And … we expect the same thing on the Internet, the traditional advertising law to apply. But this has been forgotten, and one of the prime reasons is that a lot of the

> companies who are driving the Internet, Internet advertising and creation of commercial Web sites, are a lot of new young startup companies … who are not familiar with a lot of the traditional criteria. So we really have to cite the education aspect.

SECURITIES AND EXCHANGE COMMISSION (SEC)

The SEC has a new Office of Internet Enforcement that patrols cyberspace looking for business fraud, stock fraud and other crimes. The SEC has implemented a "Cyberforce" of more than 240 attorneys, accountants and analysts, called "Cybercops," specially trained to detect fraud while surfing the Internet. For example, in November 1998, thirty U.S. state regulators, the British Columbia Securities Commission and the Ontario Securities Commission joined together for "Investment Opportunity Surf Day," searching the Internet for investment scams.

Online defrauders want to be found by potential victims. This also affords the SEC Cyberforce opportunities to detect frauds as they are developing. In some instances, the Cybercops can bring an enforcement action before any victim loses a penny. Thus, the Internet has become a powerful tool for law enforcement as well as scam artists.

The SEC asked Congress for $150 million for its enforcement and investor education programs for federal fiscal year 2001. The agency plans to create an automated surveillance system to search public online forums, such as Web sites, message boards and chat rooms for telltale words or phrases indicating unscrupulous stock promotions. SEC investigators currently do the job manually with computer search engines.

The SEC's Enforcement Complaint Center has an e-mail hotline, enforcement@sec.gov, launched in June 1996. By early March 1999, it was receiving more than 300 fraud tips a day, up from 15 a day two years earlier. The Center's toll-free telephone hotline is 1-800-SEC-0330.

The SEC has established programs to educate investors about the risks associated with Internet securities fraud, such as posting relevant information on its Web site at www.sec.gov. The Office of Investor Education and Assistance can be reached online at help@sec.gov. The SEC warns investors to read its "Cyberspace Alert" before purchasing any investments touted on the Internet. The document can be accessed through the Investor Assistance and Complaints link at the agency's Web site.

Investors can, without charge, access company financial reports that must be filed with the SEC via the agency's Electronic Data

Gathering, Analysis and Retrieval (EDGAR) system, located at its Web site. If a company's reports are not listed on EDGAR, investors may find out from the SEC (1-202-942-8090) whether the company filed a stock offering circular under "Regulation A" or a "Form D" notice.

The SEC also lists its enforcement actions and trading suspensions on its Web site. According to John Reed Stark, Chief of the Office of Internet Enforcement, the SEC has brought over 100 Internet fraud enforcement actions since 1995 (38 in 1998).

Geraldine M. Walsh, Special Counsel to the Director of the SEC's Office of Investor Education and Assistance, testified about how enforcers and consumers can take advantage of investment defrauders' need to collect money eventually:

> For investment frauds, at some point, the scamsters want to collect money, and that's where we're able to track them down.
>
> We do run into problems, though, of people just disappearing into thin air. … [O]ne of the things that we caution investors to do, this is what our enforcers do, is when you see a Web site that looks like a scam, or if you see a Web site and you're going to invest based on that Web site, … print it right then and there. And if your server doesn't give you the date and time that the information was printed, then write it down yourself, because in two days or in two hours or two minutes, that information may not be there.
>
> So there is that phenomenon of people just disappearing into thin air. But like I said, at some point these guys want money, and that's where we're able to nab them.

NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION

Based in Washington, D.C., NASAA represents state securities law enforcers. Investors can check its Web site (www.nasaa.org) for alerts regarding particular schemes or types of investments to avoid. State regulators or consumers can check the Central Registration Depository (CRD) to determine if a broker promoting a particular stock, or the broker's firm, is registered or has a disciplinary history.

NATIONAL ASSOCIATION OF SECURITIES DEALERS (NASD)

NASD can give investors a partial disciplinary history of a broker or brokerage firm. Its toll-free public disclosure hotline is 1-800-289-9999, and its Web site is www.nasdr.com.

FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)

The Division of Compliance and Consumer Affairs of the Federal Deposit Insurance Corporation (FDIC) operates a toll-free hotline at 1-800-934-3342. Its Web site to report suspicious sites or to check them out using a consumer news link is www.fdic.gov.

The FDIC has 20 examiners who surf the Net on a part-time basis to locate bank scams.

MAIL ABUSE PREVENTION SYSTEM

A voluntary group of systems administrators from around the world, calling itself the Mail Abuse Prevention System, maintains a Realtime Blackhole List of notorious spammers — senders of unsolicited e-mail. Appearing on the list, which started in 1997 and contains about 1,400 entries, marks generators of obvious junk e-mail as spammers. Enough Internet service providers refuse to deliver e-mail produced by those on the list to separate them from about 40 percent of the online world. By-and-large, this pleases the vast majority of Internet users since the overwhelming majority of spam comes from pornography sites or individuals pitching get-rich-without-working schemes.

NEW JERSEY DIVISION OF CONSUMER AFFAIRS

The New Jersey Division of Consumer Affairs (www.state.nj.us/lps/ca/home.htm) has a specialized E-Commerce Investigative Unit, also known as “cybercops,” drawn from the Division’s sub-units, including the Office of Consumer Protection, the New Jersey Bureau of Securities and the Office of Professional Boards. The Unit was established in 1995 and is headed by a supervising investigator. Ten investigators work on a full-time basis to uncover fraudulent e-commerce, including, but not limited to, securities fraud, prescription legend drug fraud, deceptive cyber-practices in the sale of merchandise and unlawful offers of professional services over the Internet. The Division’s cyber-unit has expanded its operations to join with the Division of Gaming Enforcement to combat cyber-gaming, the Division of Civil Rights in fighting discriminatory housing rentals and the Division of Criminal Justice in fighting the distribution of illegal drugs, including the date rape drug, GHB.

In March 1999, the Division implemented an online complaint form that can be completed and electronically mailed at the touch of a button. Prior to this, investors seeking to report suspicious investment offerings made on the Internet had to download the Bureau’s complaint form, complete it by hand and mail it to the Bureau.

In addition to inquiring at the SEC, investors should check with New Jersey's Bureau of Securities to see if it has additional information. The Bureau can check the Central Registration Depository (CRD) to determine whether the broker touting the stock, or the broker's firm, has a disciplinary history. It can also find out whether the offering has been cleared for sale in New Jersey.

The Bureau's surveillance efforts have led to the resolution of registration or regulatory transgressions without the need for formal enforcement action. During 1999, nearly 20 entities offering investment products or services on the Internet have registered or modified or deleted their Web sites in response to Bureau contacts. In April 1999, the Bureau assessed civil penalties for violating New Jersey's securities laws against an unregistered Internet investment adviser who misled 10 investors into making risky investments. He was ordered not to apply for registration as a broker-dealer, agent or investment adviser in the state. Also, in October 1999, the Bureau sued a company offering unregistered shares of stock over the Internet. Allegedly, five defendants pocketed more than $850,000 in net proceeds from the sale of shares to state residents.

The Cyberfraud Unit also works in other areas under the jurisdiction of the Division of Consumer Affairs. For example, on February 16, 1999, investigators assigned to the Unit conducted the Division's first "Surf Day," identifying suspicious Web sites involving licensed professionals. Many were operating without proper licenses. Several had prior disciplinary histories or failed to list proper specialty designations or permit numbers.

In late 1999, the Division filed two civil cases under New Jersey's Consumer Fraud and Pharmacist Licensing laws involving illicit sales of the drug Viagra over the Internet. In one case the anti-impotence drug allegedly was shipped in response to a request over the Internet in the name of an investigator's dog. In the other case two men who were not pharmacists allegedly offered Viagra over the Internet and dispensed it when supplied with physician prescriptions. Allegedly, in neither case did the purveyor take note of any other medications the "patient" was taking and warn of potentially harmful interactions. Meanwhile, one recent federal investigation turned up 86 Internet sites offering Viagra without a prescription.

In March 2000, the Division filed a second round of complaints against eight unlicensed pharmacies, based in six cities outside of New Jersey, for allegedly selling medication over the Internet to New Jersey patients. The companies specifically were accused of failing to disclose to undercover investigators posing as online patients that they were not licensed in New Jersey. Doctors working with the companies allegedly prescribed medication in "virtual visits,"

although they were not licensed to practice medicine in New Jersey. The “visits” required the patient to fill out a simple questionnaire but included no medical examination.

The U.S. Food and Drug Administration estimates that there are in excess of 400 online pharmacies. According to the market research firm Cyber Dialogue, more than 200,000 people bought prescription drugs online from July 1998 to July 1999. The drug mills in the profession hurt legitimate online pharmacies that work with reputable physicians and have a genuine concern for patient safety. In December 1999, the National Association of Boards of Pharmacy (www.nabp.net) established a voluntary certification program for Verified Internet Pharmacy Practice Sites™ meeting the requirements of 17 review criteria. Certifications have been awarded to *Family*Meds.com, Drugstore.com, Merck-Medco Rx Services and PlanetRx.com.

State medical and pharmacy boards have expressed concerns to the FTC that their existing enforcement tools are not adequate to police online sales of medication. In mid-1999, the FTC recommended that Congress consider whether legislation requiring disclosure of identifying information about the location of prescription drug Web sites, online prescribing physicians and online pharmacies is necessary to assist state law enforcement efforts.

In December 1999, the President asked Congress to give the Food and Drug Administration (FDA) the power to review and certify hundreds of drug-dispensing Web sites. Under the proposal, fines up to $500,000 could be levied for dispensing drugs without a valid prescription or operating without FDA certification. The FDA also would have the power to subpoena the records of online pharmacy sites during investigations. $10 million for the 2001 budget would be available to hire FDA investigators and upgrade computer equipment for the online pharmacy program. The FDA opened a consumer-advice Web page (www.fda.gov) to help patients ensure they are buying from legitimate stores instead of dangerous quacks.

Stressing the importance of jurisdiction over the activities of online pharmacies, the New Jersey Division of Consumer Affairs has called for new legislation allowing it to license out-of-state pharmacies doing business with New Jersey residents over the Internet. Additionally, the Division formed a Telemedicine Task Force to study potential problems associated with the delivery of health care via the Internet.

Telemedicine is a health care provider’s use of electronic communication and information technologies to provide or support clinical care to a patient at a remote location. Physicians use the Internet, personal computers, satellites, video conferencing equipment and telephones in telemedicine applications. The Division is developing proposed legislation based on the Task Force’s

recommendations. The proposed legislation would create a limited license that physicians outside the State would be required to possess to diagnose or treat in-state patients through the use of electronic devices. Provisions also are being drafted that would allow physicians, including those who hold the new limited license, to e-mail prescriptions for patients.

The Division also brought a civil case in October 1999 against a Monmouth County woman who, using a variety of pseudonyms, offered to sell Beanie Babies and Furby plush toys over several online auction sites. She allegedly never delivered after collecting money for the toys and for tickets to an August 1999 Bruce Springsteen concert.

As a result of its participation in a FTC-sponsored “Surf Day,” the Division brought an action against a Paterson-based credit-repair business operating via the Internet. The Division also has issued warnings to nearly 20 dentists and chiropractors in connection with irregularities in their Internet advertising. In addition, the Division published a notice in a trade newsletter, *NJ Car*, warning automobile retailers to follow proper Internet advertising practices. Moreover, prompted by consumer complaints about online auctions, the Division has requested and received information from eBay, Inc. in accordance with the latter’s policy to share information with law enforcement.

In the area of charitable fundraising, two previously unregistered charities have registered after investigators discovered that they were soliciting donations via the Internet. After the Division contacted it, a Vermont organization, Volunteers for Peace, added a disclaimer page to its Web site to make it clear that the charity was not soliciting in New Jersey, where it is not registered.

In the fall of 1999, desktop high-speed Internet connections were installed for investigators in the Office of Consumer Protection. This has enabled the Division to accelerate investigator training and to expand its focus from businesses that use the Internet as one of many tools to deceive to those that exist primarily to take advantage of e-commerce as an end unto itself. The Division specifically intends to participate in training programs offered by the National White Collar Crime Center. Moreover, efforts to educate the public about Internet fraud have been incorporated into the Division’s consumer outreach program.

IDENTITY THEFT

AN ESPECIALLY EGREGIOUS FRAUD

Identity theft undermines confidence in the integrity of commercial transactions and invades individual privacy. The Internet provides to perpetrators low-cost, efficient methods for capturing the identities of unsuspecting victims.

Sometimes called “true-name fraud” or “account takeover fraud,” identity theft commonly refers to a host of frauds, thefts, forgeries, false statements and impersonations involving the use of another person’s identifying information. Identity theft facilitated by the Internet will grow as electronic commerce grows, which it is doing exponentially. Cyber Dialogue, a New York-based Internet research company, reported that by the third quarter of 1999, 19.2 million U.S. adults had used their credit cards for online transactions, versus 9.2 million during all of 1998. The number of people worldwide buying goods and services on the Internet should rise to 120 million in about three years.

Once armed with an individual’s personal information, identity thieves use it to open new accounts, take over old accounts, make purchases or commit offenses in that person’s name. With a birth date and an address an identity thief can obtain a birth certificate and progress to obtaining a passport, driver’s license and credit, all in someone else’s name.

While impersonating another, a wrongdoer can take out loans, lease cars, buy merchandise, take trips, open bank accounts, cash checks, obtain credit cards, sign up for cellular telephone service, rent apartments, or acquire a home mortgage or equity loan. The perpetrator can saddle an innocent victim with a criminal arrest record or commit motor vehicle violations in the victim’s name.

Privacy concerns and fear of credit card fraud discourage online purchasing. Nonetheless, most experts contend that consumers are at much greater risk using credit cards at stores, restaurants or gas stations than at secure Web sites. Encryption technology and Web site authentication procedures ensure the security of online transactions to most consumers’ satisfaction. Indeed, the National Consumers League’s Internet Fraud Watch has not received a single complaint of someone’s credit card number being stolen while transmitted to a legitimate merchant over the Internet.

A couple of recently exposed incidents have diminished the absolute confidence with which many consumers conduct e-commerce via credit cards. In December 1999, an Eastern European hacker, using the alias Maxus, allegedly stole the numbers of about 300,000 credit cards from the database of an Internet Web site, CD Universe. When the firm refused to pay a $100,000 extortion demand, about 25,000 numbers were sold on a Web site, which has since been taken down.

In December 1999, British hackers attempted to extort $10 million from VISA International after obtaining access to the company's computer system in July 1999. The firm maintained that the hackers accessed some corporate servers and obtained some marketing material but no credit card or transaction processing information. With apparent confidence in its security system, VISA refused to pay the demand and contacted Scotland Yard and the FBI.

Neither of these incidents involved a successful attack on data in transit from customers to vendors or transaction processors. Secure socket layer (SSL), the security protocol built into most Web browsers, very effectively, if not perfectly, protects such data in transit. However, when companies store consumer credit information in areas that are connected to the Internet, they are asking for trouble, unless they have installed state-of-the-art security measures.

Storing credit card information in a database typically is done as a convenience to customers, but without proper safeguards, it may involve security risks. If credit card information is stored, it should be encrypted using the latest technology. Access to the database should be severely restricted, and electronic "keys" should be changed frequently. Vendors also must make sure that their own computer staffs do not abuse the credit card information. As an extra precaution, consumers may ask vendors not to save their credit card numbers, or they may use a separate credit card for online purchases only and cancel it at the first sign of vendor trouble.

Recent technological advances also are making bank account debit transactions more secure. A Woodcliff Lake-based private network owned by several large banks has developed a CD-ROM the size of a card to securely authorize withdrawal of funds from a checking account to pay for Internet purchases. Encrypted information from the "card" is routed from the customer's computer through the network to the online merchant. Once the information is confirmed, including the personal identification number (PIN) entered by the customer, the money for the purchase is automatically debited from the customer's checking account. Because of the strength of the encryption, a cyber-thief would have to steal the actual "card," along with the customer's PIN, in order to access his checking account. No financial data is actually typed into a keyboard or sent to a merchant's Web site and stored.

Banks and credit card companies pick up the lion's share of the

direct financial tab for identity theft. Under the Fair Credit Billing Act, an individual's financial liability is limited to $50 if he promptly reports fraudulent use of a credit card to the credit-card company. For similar protection, debit-card holders must notify their banks within two business days. If they wait longer, users are liable for as much as $500. Meanwhile, the corporate victims pass their losses on to consumers, who bear the costs indirectly in the form of higher prices and interest.

The indirect financial and "human" costs of identity theft for the individual victim are quite substantial. People whose identities are stolen must cope with reputations for substantial indebtedness, ruined credit histories, difficulty finding employment, and trouble renting or buying housing. For many victims, their only "fault" was being on a list or in a file that was stolen, or being duped into giving out information to the wrong people.

A victim may not even know that her identity has been stolen until she is dunned for a debt about which she knows nothing. Meanwhile, her credit reports, in the hands of national commercial credit bureaus that report creditworthiness to vendors and lenders, may contain errors for a number of years before they are fixed. Unless the credit reporting companies promptly correct the information in their files, the victim may have to continuously establish the creditworthiness that other consumers take for granted.

Recent federal legislation allows consumers to seek restitution for expenses from the criminal who carried out the identity fraud. However, actually obtaining such restitution might prove impossible if the criminal is not caught or if there is a long list of creditors seeking similar restitution.

The significant financial losses incurred by identity theft victims trying to restore equilibrium in their lives have prompted at least one national property casualty insurer to offer identity fraud expense coverage, starting in 1999. Available to homeowner and tenant policyholders for an additional premium of about $25 per year, the coverage reimburses victimized policyholders for up to $15,000 in expenses they incur as a result of identity fraud. Expenses covered include legal expenses, loan re-application fees, telephone and certified mailing charges, notary expenses and lost wages for time taken from work to deal with the fraud.

Although the volume of identity fraud in the United States and New Jersey is difficult to quantify, available information indicates that it is prolific, and undoubtedly one of our fastest growing crimes. Loss prevention experts believe 20 people have their identities stolen in New Jersey every day. MasterCard International reported that identity theft accounted for $1 billion in losses in 1998.

Officials do not have comprehensive figures on how many identity thefts occur annually because it is not broken out as a separate crime in analyses of fraud schemes. The U.S. Secret Service's national tracking reveals that at least 1,000 Americans are victimized by identity theft every day and that the cost almost doubled from about $442 million in 1995 to $745 million in 1997. According to the Public Interest Research Group (PIRG), up to 40,000 people are victimized by identity theft every year.

Trans Union LLC — the only credit bureau to track identity theft cases — reported that two-thirds of all consumer inquiries to its Fraud Victim Assistance Department involve identity theft, according to a 1998 General Accounting Office study. The number of cases reported to Trans Union's hotline jumped from 35,235 in 1992 to 522,922 in 1997, the GAO added. Another credit bureau, Equifax Credit Information Services, Inc., received 1,200 calls a day on its fraud lines in 1997, quadruple the number received in 1995. In 1996 and 1997, identity theft was the number one complaint at the Privacy Rights Clearinghouse, based in San Diego, California.

Meanwhile, the Social Security Administration, which operates a fraud hotline at 1-800-269-0271, reported that it received 30,115 complaints about the misuse of Social Security numbers in 1999, most involving identity theft. That was a tremendous surge from 11,013 such complaints received in 1998 and 7,868 in 1997.

It is easy to understand why so many criminals, including organized rings, have turned to identity theft in ever increasing numbers in modern times. An identity thief runs up an average of $20,000 to $30,000 in bills on each victim versus the average take from a more risky bank robbery of just $2,500.

Retrieval of identity information via the Internet is just the most recent of many methods by which perpetrators compromise others' identities. According to the U.S. Secret Service, organized groups account for 75 to 80 percent of identity fraud cases. Members of the rings get jobs with housekeeping companies or security firms and then snoop for sensitive information in computers, file cabinets and trash bins. In March 2000, for example, Union County authorities arrested 14 people connected to an organized crime group whose main operation was identity theft. Allegedly, an auto dealership employee provided to the group's leader driver's license information for customers taking test drives or applying for financing. Using high-tech methods to reproduce official documents, the group allegedly created hundreds of phony driver's licenses used to apply for credit cards and instant credit at electronic and home improvement stores. In some cases, merchandise obtained by impersonators allegedly was sold — sometimes over the Internet — to pay off their debts to at least one loan shark associated with the group.

The Internet now affords perpetrators, whether operating individually or as members of organized rings, access to a vast amount of information about individuals and businesses with just a few keystrokes. Until 1997, the *Congressional Record's* Web site included the Social Security numbers of military officers granted promotion approval by Congress. Using the data on the government Web site, a private site operator posted the numbers, along with those of many prominent public figures. In December 1999, the Newark Office of the Secret Service arrested three people for allegedly using the military officers' numbers to create hundreds of phony credit card accounts, including at least one in the name of the former Chairman of the Joint Chiefs of Staff. Two Trenton residents pled guilty in U.S. District Court in early 2000.

If an identity thief wants someone's Social Security number, he or she can purchase it from one of a host of vendors selling personal information on the Internet. The ready availability of Social Security numbers in the public domain has enabled at least one Web site, docusearch.com, to offer to retrieve a person's Social Security number in one day for a $49 fee.

Many legitimate companies obtain significant amounts of personal information about Internet users and their children in order to pass it on to marketers selling merchandise or services via e-mail or advertising banners. In return for permission to collect and distribute information about purchasing preferences and household demographics, these companies offer incentives ranging from the opportunity to win scholarships in sweepstakes to cash payments for each e-mail received. If not careful, however, a person could respond to a phony offer and provide information that could be used for identity theft or other illicit purposes.

The human element is the weakest link in the information security chain. Violators take advantage of human carelessness through high-tech and low-tech snooping. Traditional methods include sorting through discarded trash ("dumpster diving"), co-workers or cleaning crews rifling through workplace desk drawers, theft of U.S. mail, bribing bank employees, and soliciting information with false job application schemes. With these methods exposure is limited, however, by the physical process required to gather the information. Online, on the other hand, aggregation of personal data can occur rapidly as the perpetrator surfs from source to source with a few keystrokes and without ever having to leave home.

With inexpensive but sophisticated "desktop publishing," criminals can quickly create high-quality false identity documents or checks in someone else's name. In the case of Internet transactions, the wrongdoer does not have to present bogus identification documents, whose falsity sometimes can be detected by careful inspection.

Criminals compromise real identities far more often than they fabricate new ones. Thieves can capitalize immediately on a business's confidence in a longstanding relationship with a reliable customer. The defrauder does not have to cultivate a new relationship with the corporate victim.

It is likely that the private sector will, in the long run, resort more and more to definitive methods for confirming consumer identity: fingerprints, iris scans, face-recognition software, so-called "smart cards," and the like. IriScan, Inc. (www.iriscan.com) of Marlton, New Jersey, for example, has developed iris recognition technology for automated biometric systems. Visionics, Inc. of Jersey City, New Jersey, developed software called FaceIt whose uses include identification of customers at ATM machines via their distinctive "face prints." This helps people who lack bank accounts but wish to cash checks. The company reported that about 645,000 people have registered their face prints to cash checks and wire money at 500 Wells Fargo face recognition ATM machines in California, Texas, Arizona and Florida. However, organizations such as the Online Privacy Alliance (www.privacyalliance.org) and PIRG reject such methods as invasion of privacy.

Law enforcement officials and privacy activists believe that credit card companies and banks already have substantial "know-how" to prevent a large portion of fraud and counterfeiting but are reluctant to invest in the technology or assign the necessary resources. When a "customer" requests a change of address, for example, the company extending credit always should communicate with the customer of record at the old address or telephone number in order to confirm the change. Sometimes, careless lenders even permit transactions on closed credit card accounts.

Creditors and credit bureaus could implement a fraud notification system that would use software to identify patterns of fraudulent use within the creditor or credit bureau's databases. Once suspicious transactions were flagged, timely notification could be given to all interested parties, including the individual victim.

Most credit card issuers claim they already vigilantly monitor customers' buying patterns and quickly flag questionable transactions. Several of the country's largest credit card issuers are now building a database, with assistance from the Secret Service, in order to share information and identify common geographic locations where credit card fraud occurs.

Although Post Office "mail drops" are essential for the success of many schemes, including credit card and identity theft, in the past there was little scrutiny to determine if they were being used for illegal activity. Effective April 24, 1999, new U.S. Postal Service

regulations imposed stricter requirements on private mailbox (PMB) customers and commercial mail receiving agencies (CMRAs). The latter are private businesses that, through a written agreement, accept their customers' mail from the Postal Service, hold it for pick-up (private mailbox) or re-mail it to other addresses.

Under the new regulations, CMRAs must register with the Postal Service to act as an agency to receive delivery of mail for others. They must ask those who rent PMBs from them to produce two forms of identification, one with a photograph. They may not deliver mail to a box unless the customer has identified himself in a Form 1583 that is kept on file. The CMRAs are required to submit quarterly alphabetized lists of their customers to the Postal Service. Their customers must use the designation "PMB" and the relevant number in their mailing address. An address format change will let correspondents know they are dealing with the holder of a private mailbox at a specific street address and not an occupant of a "suite" or "apartment."

A large share of the responsibility for identity theft rests with the credit card issuing companies and vendors who extend credit too eagerly. Pre-approved credit card applications abound in everyone's mail and e-mail. John P. Lucich, President of Secure Data Technologies Corp. of Fairfield, New Jersey, testified that his seven-year-old son recently received one. Beth M. Grossman, the Federal Trade Commission's Identity Theft Program Manager, testified that Department store chains constantly seek customers who will open a chain credit account in return for a discount on a current purchase. She added that in their zeal to grant credit instantly they do not check the customer's credit report, which might contain a fraud alert. By failing to check, they provide additional opportunities for identity thieves.

DEMONSTRATION OF ONLINE PITFALLS

Pretending to sell products and services, fake Web sites entice customers with attractive looking deals. They ask the unsuspecting victims for their names, addresses, credit card numbers and mothers' maiden names. Sometimes the consumer will provide the information in connection with an application for credit from a sham credit card site. The site's operators e-mail the consumer that her application has been denied and simultaneously provide her personal information to identity thieves.

John Lucich testified how a defrauder could turn a credit card with a simple $1,000 credit limit into an illicit cash cow. Armed with such a card under a phony or stolen identity, the perpetrator applies for a credit card processing machine commonly advertised in magazines for use by home businesses. The defrauder then obtains a legitimate

merchant’s credit card processing number and terminal ID number from discarded receipts that he might find lying around a mall parking lot. He programs the numbers into the credit card processing device. Then, he makes purchase after purchase with the credit card. However, he never exceeds the card’s credit limit because he uses the processing terminal and the impersonated merchant’s numbers to enter returned merchandise credits canceling the charges in the credit-card company’s computer. By the time the credit-card company realizes what has happened, the perpetrator, enriched by material goods from several expensive purchases, is long gone.

Mr. Lucich pointed out that “[a]nybody can set up a Web site for as little as $15 and attempt to defraud people.” Through online financial newsgroups, the scammer can find out the e-mail addresses of people interested in enhancing their credit. He then spams such people with e-mail touting the easy availability of credit on his Web site. Once lured there, they provide the information that allows the perpetrator to steal their identities and leech their good credit histories. In that way, the schemer can reach thousands or even millions of specifically targeted potential victims with the click of a mouse. It would take months, a large staff and significant expense to reach such an audience with traditional solicitation by telephone or so-called “snail mail.”

Pretending to be a consumer, Mr. Lucich showed how a phony Web site dupes unsuspecting credit seekers. In a search engine for the aviation industry, he pointed out a rotating advertising banner offering a credit card with an especially low interest rate. By clicking on the banner, the “consumer” could view a Web site that usurped the logos of legitimate credit card providers, such as Visa and MasterCard, and displayed an application form. The site also contained a reassuring, but fake, certification of security and an offer of a free credit report. The application form asked for personal information, such as date of birth, social security number and mother’s maiden name, as well as numbers and expiration dates of existing credit cards. When Mr. Lucich submitted the completed application, the screen displayed the message: “Currently … our Web servers are overloaded. Please try again at a later time. Thank you for your patience.” Although the “consumer” believes that his completed form was never sent, a defrauder has now captured all his pertinent credit information.

The FTC’s Beth Grossman testified how even a vigilant credit card company can be duped by a thief armed with an individual’s identifying information. The thief starts by telephoning the company to change the address on the account. Armed with his victim’s personal information, the thief can answer all of the questions asked by the company’s representative to separate genuine customers from wrongdoers. The thief knows the legitimate customer’s social security number, date of birth and mother’s maiden name. Once the company assigns a new address

to the account, the thief can order expensive items with impunity, collect them at various delivery addresses, and never have to fear timely interruption by authorities tipped off by the victim. Discovery of the scheme occurs only when substantial monthly bills are not paid or bogus credits from an impersonated vendor are discovered. When the true account holder is traced back to his original address, the impersonator and his purchases are long gone. Ms. Grossman added, "The frustration happens when people don't find out about this until it's at the time they need credit. They go to get a mortgage or student loan, and they find that their credit is all screwed up."

HOW TO AVOID BECOMING A VICTIM

A simple guideline is to assume that no personal information is absolutely private or safe. Anthony F. Colgary, Assistant to the Special Agent in Charge of the U.S. Secret Service's Newark Field Office, testified potential victims "bear some responsibility to try to monitor [their] credit reports to see what's going on." He added:

> No credit can be gained in your name, whether it's a credit card or anything else, unless someone passes a credit check on you. You need to constantly review that credit report and make sure that no one has changed your address, no one has ordered goods or services or credit that you haven't authorized ….

People may protect themselves from identity theft by taking the following steps:

- Get a free copy of your credit report from each of the three major credit bureaus every year. Check to be sure that everything, including addresses, is accurate. Under the federal Fair Credit Reporting Act (amended by the Consumer Credit Reporting Reform Act of 1996), a consumer who has been denied credit during the last 60 days may receive a free copy of his credit report. In New Jersey he is entitled to one free copy annually, even if he has not been rejected for credit. The cost is about $8.00 for each additional report.

  To order credit reports from the three largest credit bureaus, contact Equifax, Inc. (1-800-997-2493) (or 1-800-685-1111) (www.equifax.com); Trans Union LLC (1-800-916-8800) (www.tuc.com); and Experian (www.experian.com) (1-888-397-3742) (formerly TRW).

- Monitor your account activity throughout the year by reading your periodic statements thoroughly.

- Tear up or shred any pre-approved credit offer, receipt or other

personal information that links your name to an account number. Do not leave your ATM or credit card receipts intact in the trash. If you decide not to proceed with a loan or purchase, take all unused copies with information home with you. Destroy or delete social security numbers from any documents before throwing them away.

- Credit card solicitations are generated from "pre-screened lists" of credit reports provided by credit bureaus. If you do not want to receive these offers, contact each of the Big Three credit bureaus to remove your name from pre-screened lists.

- If your credit card or other bills are more than two weeks late, do three things: First, contact the Postal Service to see if someone has forwarded your mail to another address. Second, contact your bank to ask if the statement or card has been mailed. Third, contact the businesses that send you bills.

- Do not pay your bills by putting them in your home mailbox with the red flag up. Use the Post Office or a postal mailbox for bill payments. Protect your incoming mail with a locked mailbox or Post Office box.

- Protect your account information. Do not write your personal identification number (PIN) on your ATM or debit card. Do not print or write your social security number, credit card account numbers or driver's license number on your checks or on the outside of envelopes when paying monthly bills. Cover the pad when you are entering PIN numbers.

- Do not carry your social security card, passport or birth certificate unless you need it that day. Take all but one or two credit cards out of your wallet, and keep a list in a safe place at home of your account information and customer service telephone numbers. Keep tax records and other financial documents in a secure place.

- Memorize your social security number and all passwords and PIN numbers. Do not use common identifiers, such as mothers’ maiden names and birth dates, as passwords or PIN numbers.

- Never provide personal, credit card or other financial information over the telephone or online, unless you initiate the contact. In a New Jersey case in January 2000, four students at Absegami High School in Galloway Township allegedly purchased about $8,000 in merchandise, delivered to unoccupied homes, using credit card numbers obtained by tricking America Online and Earthlink subscribers. The teenagers allegedly acquired passwords, addresses, telephone numbers and credit card numbers

of people in New Jersey and at least six other states by, in some cases, posing as online representatives of the service providers. They told the subscribers that their account information had been lost and should be provided again.

- Cancel, in writing, any credit cards that you do not intend to use.

- If a “creditor” contacts you, do not provide information about your account without contacting the creditor via a telephone number, address or e-mail address indicated on your monthly statement.

- Do not put your genealogy online. It permits identity thieves to acquire birth dates and maiden names.

- Check social security earnings and benefits statements once a year to make sure the earnings are recorded correctly.

- You may want to have your name, address and phone number deleted from marketers’ lists. Write to the Direct Marketing Association’s Mail Preference Service (PO Box 9008, Farmingdale, NY 11735) and Telephone Preference Service (PO Box 9015, Farmingdale, NY 11735).

ACTIONS VICTIMS MAY TAKE

Despite precautions, growing numbers of individuals fall prey to identity theft. Early detection and reaction is essential to minimize the harm. It is important to quickly take the following actions:

- Immediately, make a complaint to your local police department. Obtain a written copy of the police report for inclusion with notification letters. Contact the Federal Trade Commission to report the problem at 1-877-FTC-HELP.

- Immediately telephone the toll-free hotlines for the fraud units of all three major credit bureaus and ask them to "flag" your account with a “Fraud Alert/Victim Impact” statement. This tells creditors that you are a victim of identity fraud and asks them to contact you before opening any new accounts. The major credit bureaus’ fraud unit telephone numbers are Equifax (1-800-525-6285), Experian (1-800-397-3742) and Trans Union (1-800-680-7289). Follow up in writing, attaching a copy of the police report. The addresses are Equifax (P.O. Box 105069, Atlanta, GA 30348), Experian (Attn: Consumer Assistance Department, CBA Information Services, P.O. Box 677, Cherry Hill, NJ 08003) and

Trans Union (P.O. Box 6790, Fullerton, CA 92834).

- Order a copy of your credit report. The report is free if you are a victim of identity theft or have been denied credit in the last 60 days. Anytime you apply for a loan of any type, you are entitled to a copy of the credit report that is provided for you.

- Immediately notify your banks and obtain new account numbers for all of your checking, savings and other accounts. Pick new PIN numbers for your ATM and debit cards. Close all of your credit card accounts and reopen them with new numbers.

- Immediately notify affected creditors by telephone and follow up with written notification enclosing a copy of the police report.

- Immediately notify your local postmaster. Explain that you suspect a false address is being used and would like help to find out the address. Also notify the U.S. Postal Inspection Service (Web site located at www.usps.gov/postalinspectors) of any suspected mail theft or use of impersonating addresses.

- Call the local field office of the U.S. Secret Service to report any credit card fraud.

- Call the Division of Motor Vehicles to see if another license was issued in your name. Put a fraud alert on your license. You may want to request a new number.

- Contact the Social Security Administration's Fraud Hotline: 1-800-269-0271. Depending on the circumstances, you may want to obtain a new social security number from the Social Security Administration. You also may want to contact your local telephone, long distance, water, gas and electric companies to alert them that someone may try to open accounts in your name.

- Maintain a log of all contacts with authorities regarding the matter. Write down each person's name, title and phone number. You may need to re-contact them or refer to them in future correspondence.

- Do not allow yourself to be coerced by creditors into paying fraudulent bills.

RECENT LAWS AND CONTROL PROGRAMS

Recently, special laws to contend with identity theft have passed at the federal level and in New Jersey. Previously, criminal

prosecutions were limited to fraud, theft, forgery and impersonation charges associated with the identity theft. Victim loss thresholds of $40,000 or more limited the number of offenses brought to court.

NEW JERSEY LAW STRENGTHENED

Effective May 21, 1999, *N.J.S.A.* 2C:21-17, concerning wrongful impersonation, was amended to specifically include identity theft in its provisions. Before the amendments became law, the offending conduct had to fit the elements of theft by false representation before it could be prosecuted criminally. The amendments also allow authorities in New Jersey to prosecute those who make purchases in another state using identity information from a New Jersey resident. Gerald S. Flanagan, Legislative Director for New Jersey Public Interest Research Group (NJPIRG) Citizen Lobby, testified that an effective state law was needed because the majority of consumer prosecutions take place on the state level.

FEDERAL LAW STRENGTHENED — ENHANCED ROLE FOR FTC

The federal Identity Theft and Assumption Deterrence Act of 1998 took effect on October 30, 1998. The new law makes it a separate federal crime to use someone else's social security number, date of birth, mother's maiden name or other identifying information to commit fraud or engage in other unlawful activities. It recognizes as a victim the person whose identity is stolen. It permits the victim to seek restitution in court and imposes penalties based on how much was stolen with the false identity. The federal Sentencing Commission has examined what non-monetary factors should be considered in determining the appropriate sentence for an identity thief.

The new law requires the Federal Trade Commission (FTC) to establish a centralized identity theft complaint center, similar to Consumer Sentinel, to provide information to consumers, referrals to law enforcement and advisories to credit reporting agencies. On November 1, 1999, the FTC launched a special toll-free, identity theft hotline, 1-877-ID THEFT (438-4338), where people can register complaints and obtain information about identity theft. A complaint form is available at www.consumer.gov/idtheft. The FTC also may be contacted at www.ftc.gov or its Consumer Response Center: 1-877-FTC-HELP. The agency has published a free brochure, "A Consumer's Guide to Travel in Cyberspace: Site-Seeing on the Internet."

OTHER CRIME-FIGHTING FEDERAL AGENCIES

The U.S. Secret Service (www.treas.gov/usss) is a law enforcement

bureau within the Department of Treasury. Historically, it has investigated crimes that have interfered with evolving payment methods, from cash to plastic and electronic media. In 1982, with the passage of the Comprehensive Crime Control Act, the Secret Service expanded its investigative mission to include the manufacture and distribution of identity documents, such as social security cards, state driver's licenses, birth certificates, passports/visas, voter registrations and alien registrations.

While the Secret Service has primary jurisdiction for investigations involving credit card fraud, no federal agency has overall jurisdiction regarding identity fraud. Various federal agencies can investigate it as a crime in its own right under the Identity Theft and Assumption Deterrence Act of 1998 or as enabling conduct that results in other crimes over which they have jurisdiction. In the past, federal agencies concentrated their enforcement efforts on crimes for which the theft of identity information merely served as a predicate. These crimes include fraudulent use or production of identity documents (18 *U.S.C.* §1028), access device fraud (§1029), computer fraud (§1030), wire fraud (§1343), economic espionage (§1831), money laundering (§1956), mail fraud, social program fraud, bank fraud and tax refund fraud.

With the U.S. Secret Service as the lead agency, a West African Task Force was formed recently in New Jersey to counter identity theft. Other agencies in the Task Force are the FBI, the State Department, the INS, the IRS, the U.S. Postal Inspection Service, the Inspector General of HUD, the New Jersey State Police and prosecutors' offices in Union and Essex counties. There are similar task forces in other states, and agents are assigned to the U.S. Embassy in Nigeria. In 1998, the New Jersey Task Force generated 31 federal and 62 county prosecutions.

The U.S. Postal Inspection Service (www.usps.gov/websites/depart/inspect) focuses on methods of identity theft involving the mail. It publishes a *Credit Card Mail Security Newsletter* for law enforcement.

KEEPING PERSONAL INFORMATION PRIVATE AND ACCURATE

Preservation of privacy has become more important in today's world of instant access to electronic data. Property deeds and court case data, complete with unlisted telephone numbers and other personal information, used to be available solely to individuals who were familiar with complicated county recording systems. Now much of that information can be found on the Internet. Computerized database services (sometimes called "individual reference services" or "look-up services") are used widely by both public and private sector entities

to locate people or to verify their identities.

There are few laws restricting the collection and distribution of personal data. Such information has been released continuously to marketers, database managers and others via mailing lists supplied by commercial entities and various state and local government agencies. In 1997, there was an outcry when the Social Security Administration implemented a short-lived program to make personal earnings and benefit records available on its Web site.

Such concerns led to the passage in 1994 of the federal Driver's Privacy Protection Act. The law forbids states from disclosing, without drivers' consent, addresses, telephone numbers, medical condition information, Social Security numbers, photographs and the like contained in license applications. On January 12, 2000, the U.S. Supreme Court unanimously upheld the federal law. New Jersey law prohibits the sale of driver or registration information. Similar laws would ensure that even as the details of people's lives become more eagerly collected by marketers and more readily available through the Internet, widespread access would not go unchecked.

Credit reporting services (sometimes called credit bureaus) collect information and sell assessments of creditworthiness. The largest credit bureaus are Equifax, Inc., Experian (formerly TRW) and Trans Union LLC. Each has files on more than 120 million Americans. Together, they generate more than two million consumer credit reports each day. Under the New Jersey Fair Credit Reporting Act, effective January 27, 1998, anyone requesting a person's credit report has to state the purpose for the review — for example, renting an apartment or processing a loan application. An employer may not obtain a consumer report on a prospective employee unless that person has authorized the procurement of the report in writing.

The credit bureaus provide a valuable service by giving lenders the confidence to extend credit. However, their files often contain a great deal of personal information that is valuable to identity thieves or that can be compromised by impersonation activity. Consumers should, therefore, carefully monitor their consumer reports for accuracy and any unauthorized activity. New Jersey law permits a consumer to receive an annual free report from any consumer reporting agency.

New Jersey PIRG's Gerald Flanagan testified how online vendors have increased substantially the dissemination of personal information:

> [O]ne of the intents [of an online business] is obviously to sell a product. Number two is to establish a list of potential consumers so they can sell it to another corporation, market, whatnot. So while … selling a product is … the expressed intent

> of the transaction over the Internet, the one that's not expressed is this intent to establish a list, a consumer profile, that they can then sell to another marketer.

Mr. Flanagan pointed out that although the consumer clearly authorizes the use of information necessary to complete the transaction, she does not thereby consent to the sale of her personal information to a party unknown to her.

Mr. Flanagan recommended restricting the information that may be collected from a consumer to that necessary to complete a transaction. He noted, however, that vendors and others obtain a great deal of personal information through sources other than direct communication with the affected individual. He recommended that government prohibit the sale of such information without the knowledge and consent of the individual.

The FTC's Beth Grossman testified that her agency has been working with major companies to encourage them to adopt online privacy policies. She advised consumers visiting e-commerce sites to check whether the sites display privacy policies. She listed what consumers should look for when they buy online:

> A good online site should have a privacy policy telling [the consumer] what information they're collecting, what they will use that information for, and giving [the consumer] a means of opting out of the sale of that information.

Ms. Grossman added that online consumers should apply some of the same good sense that they use offline: "You deal with the companies that you know. Don't provide information that you wouldn't provide to a stranger in another context."

In June 1998, the FTC reported that in its March 1998 review of 1,400 randomly selected Web sites, including 212 directed at children, at least 85% solicited some sort of personal data. Less than 2% of the sites disclosed how the information would be used. However, the Direct Marketing Association, which opposes regulation of the Internet, did a survey that showed that in May 1998, 70% of 100 popular children's sites and 64% of popular business sites posted privacy statements. This was a sharp increase from the figures of a January 1998 survey.

Nonetheless, the FTC recently began to implement regulations adopted under the Children's Online Privacy Protection Act of 1998. The law and regulations control the collection over the Internet of personal identifying information about children under age 13, especially that collected without a parent's permission. The aim is to keep such information out of the hands of people who might use it to harm or exploit children.

Under the federal Fair Credit Reporting Act, consumers and the FTC can bring actions against consumer reporting agencies and data furnishers if their information is inaccurate. The law permits consumers to receive free disclosure of their reports within 60 days of a credit, insurance or employment denial. It allows consumers to challenge the accuracy of any item of information in the report and require it to be re-verified within 30 days, or removed. The law limits access to consumer reports only to those with a permissible purpose and permits consumers to bring a civil action against anyone who accesses a report for false purposes. Lastly, it permits consumers to remove their names from credit bureau mailing lists sold to credit grantors for the purpose of making credit card offers. This allows consumers to stop receiving unsolicited "pre-approved" credit card offers.

Through its subsidiary BBBOnLine®, located at www.bbbonline.org, the Council of Better Business Bureaus (CBBB) recently developed a self-regulatory online privacy program. Businesses that post online privacy policies that meet required “core” principles, such as disclosure, choice, security and the like, receive a seal. BBBOnLine also helps to settle participating companies’ disputes with their customers. It monitors program compliance by requiring participating companies to undertake an annual assessment of their online privacy practices. Consequences of non-compliance may include seal withdrawal, adverse publicity and referral to government enforcement agencies.

The Children’s Advertising Review Unit (CARU) of the CBBB implements protections for kids’ online privacy. It specifies that vendors need to obtain parental consent before requesting certain sensitive information from children.

In 1997, the Individual Reference Services Group (www.irsg.org), a trade association of 14 of the largest information providers, including the three major credit bureaus, LEXIS-NEXIS and West’s Information America, Inc., agreed to comply with a set of self-regulatory industry guidelines. Members agreed to refrain from distributing to the general public certain personal information, such as social security numbers, mothers’ maiden names and dates of birth. Such information can be distributed to private investigators under the guidelines, and information obtained from public sources, such as DMVs, can be distributed to anyone. The guidelines prohibit the dissemination of marketing data to the public. They also prohibit the dissemination of information about children, except for cases involving missing children. The participants also agreed to undergo annual compliance reviews by an independent third party. The guidelines took effect in December 1998.

For some time, the FTC maintained that voluntary industry guidelines would control effectively the collection of personal information online. Then, in February and March 2000, the agency

surveyed U.S. commercial Web sites to determine how personal information is being collected from online consumers. In a 3-2 vote, the FTC in May 2000 approved a report on the survey results to Congress (www.ftc.gov/reports/privacy2000/privacy2000.pdf). The report, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, concluded that online businesses have not done enough to ensure privacy. It recommended that Congress enact laws setting “basic standards” for online collection of information not already covered by the Children’s Online Privacy Protection Act.

There are several patchwork bills in Congress aimed at restricting the flow of intimate personal data in cyberspace. One bill would require written consent before a computer service could disclose a subscriber’s personal information to a third party. Pending bills would require employers to inform job candidates if a background check was the reason why they were not hired. Job prospects would be able to fix bad information in a report.

A proposed Personal Information Privacy Act would prevent credit bureaus from selling lists with personal identification ("credit header") information, such as name, aliases, birth date, social security number, and current and previous addresses. The bill would permit the distribution of just name, address and phone number, if listed.

PRIVATE HELP AND PREVENTION RESOURCES

Project OPEN is a joint effort of the Interactive Services Association, the National Consumers League and leading online and Internet service companies. It has created two brochures available from the National Fraud Information Center’s Web site. They are *Making the Net Work for You: How to Get the Most Out of Going Online*, a basic primer for first-time online users, and *Protecting Your Privacy When You Go Online*, which provides basic privacy tips and advice on how to avoid fraud and abuse by safeguarding one’s personal information. Project OPEN also offers advice for consumers about "spam," unsolicited e-mail.

The Privacy Rights Clearinghouse (PRC) of San Diego is a nonprofit consumer information program and an advocacy group for fraud victims. Established in 1992, its Web site is www.privacyrights.org. Its hotline is 1-619-298-3396. Along with the California Public Interest Research Group (CALPIRG) (www.pirg.org/calpirg) the PRC developed a two-page flyer entitled "Identity Theft: What to Do If It Happens to You." The PRC recently published a 12-page guide on *Children in Cyberspace* (available on its Web site). It also issued a fact sheet, "Coping With Identity Theft: What to Do When an Imposter Strikes." In addition, it published *The Privacy Rights Handbook* (Avon

Books, September 1997), which contains hundreds of tips for consumers on how to safeguard privacy, including a chapter on identity theft.

Victims of Identity Theft (VOIT), on CALPIRG's Web site, is a support group founded by identity theft victim Elsie Strong. Harry Zuckerman wrote *Good Credit: Your Own Fort Knox* (sold over the Internet). Robert B. Gelman and Stanton McCandlish, Program Director for the Electronic Frontier Foundation, wrote *Protecting Yourself Online: The Definitive Resource on Safety, Freedom & Privacy in Cyberspace* (www.eff.org/promo/protectbook.html).

Mari J. Frank, an activist victim of identity theft, wrote *The Identity Theft Survival Kit*, which may be ordered at www.identitytheft.org. Ms. Frank also authored *From Victim to Victor*, a step-by-step guide to ending the nightmare of identity theft.

Consumers concerned about privacy of the information they supply to Web sites can look for seals from at least one of three helpful organizations. A seal from TRUSTe (www.truste.org) means a Web site has posted a privacy statement informing consumers what personal information the site gathers. TRUSTe investigates complaints about its members' sites. The TRUSTe seal does not protect consumers from problems related to the quality of products and services that are offered by online vendors.

The Electronic Privacy Information Center (EPIC) is a Washington, D.C.-based watchdog group. Its third annual "Surfer Beware" report, issued in March 2000 and on the Web at www.epic.org/reports/surfer-beware3.html, assesses the privacy practices of the 100 most popular shopping sites on the Internet. The report concludes, "Not one of the companies adequately addressed all the elements of fair information practices" outlined in privacy guidelines established in 1980 by the Organization for Economic Co-operation and Development (www.oecd.org). The underlying study also examined the use in Web site operations of profile-based advertising aimed at specific customers and "cookies," files that record users' browsing habits. Of the 100 sites studied, according to EPIC, 18 did not display a privacy policy, 35 had profile-based advertisers operating on their pages and 86 used cookies.

The Center for Media Education (www.cme.org) is a nonprofit, children's advocacy organization based in Washington, D.C. The September 1998 issue of *PC World* is dedicated to online privacy. Junkbusters Corp. (www.junkbusters.com) has frequently criticized the FTC on privacy issues but called its recent regulations on children's online privacy a "remarkably good job." To see how cookies work, visit Privacy.net, www.privacy.net, a consumer protection site. To learn how to view, manage and delete cookies, visit Cookie Central. Its Web site is www.cookiecentral.com. Privacy Companion™, free software from IDcide™, can be downloaded from www.idcide.com. It works with an

Internet browser to alert users when they are tracked on the Internet and by whom. Users can decide how much information they want to give away in order to benefit from personalized services.

INTERNET GAMBLING

OFFSHORE FIRMS SERVE A GROWING DEMAND

Despite questions about its legality in the United States, Internet gambling (sometimes referred to as cyber-gambling, “nambling,” virtual gambling or interactive gambling) is growing exponentially. It offers all forms of gambling to every online household 24 hours a day. Via the Internet, betters can indulge in casino-style gambling, such as blackjack, poker, slot machines and roulette. They can bet on sports, horse or dog races, lotteries, bingo, tournaments, election results, sweepstakes and more. Many observers believe that online trading in the stock market, especially so-called “day trading,” is nothing more than gambling on stock market performance.

On May 31, 2000, the Assembly Commerce, Tourism, Gaming and Military and Veterans’ Affairs Committee held an informational public hearing on Internet gambling. Several witnesses compared prohibition of the industry to regulation and expanded on why they preferred one or the other. The Committee gathered facts from experts but made no official recommendations. A transcript of the public hearing will appear at www.njleg.state.nj.us/html/legdocs.htm.

Long distance wagering has attracted the gambling public for a long time. Currently, seven states permit the taking of bets on horse races over the telephone from bettors in other states. Two permit betting on horse races via computer. It may be possible one day to buy lottery tickets over the Internet 24 hours a day.

The National Gambling Impact Study Commission (www.ngisc.gov) reported in June 1999 that Sebastian Sinclair, a research consultant for Christiansen/Cummings Associates, Inc., estimated that Internet gambling more than doubled from 1997 to 1998. He concluded that the number of Internet gamblers worldwide increased from 6.9 million to 14.5 million and that Internet gambling revenue rose from $300 million to $651 million. Mr. Sinclair estimated that such revenue would reach $2.2 billion this year. Some market analysts predict that Internet gambling volume could reach $6 billion by 2003. By comparison, 450 commercial casinos in the United States had gross revenues totaling $20 billion in 1998, while American Indian casinos brought in $7.2 billion, according to the American Gaming Association.

Although there is no central registry of Web sites offering betting, most experts believe there are more than 850. The January 26, 1998 issue of *Sports Illustrated* noted that Internet sports-gambling sites increased from two in 1996 to more that 50 by 1998. On February 1, 1999, the Web site *Rolling Good Times* listed 110 sports-related Internet gambling sites.

By and large, Internet gambling providers have been confined physically to locales outside the United States, but Americans have easy access to their services via the boundless Internet. Most of the cyber-gambling Web sites are located in the Caribbean, Australia and continental Europe. Some are fly-by-night, unregulated operations and some are under limited foreign regulatory control or government ownership.

Unregulated or poorly regulated Internet gambling operators can abuse their customers with little accountability. Operators can alter, move or entirely remove their sites within minutes, running away with credit card numbers and money from deposited accounts. To counter such abuses, several Web sites currently assess the pay out activity of Internet gambling operations and rate them for reliability.

When a game of chance's results are not tied to the outcome of a public event, such as a horse race or a sports contest, an Internet gambling operator can manipulate the software to achieve a result which unduly favors the operator at the expense of its customers. Inadequate or missing regulation enables dishonest operators to tamper with results with impunity.

Some operators do little to scrutinize the age of online bettors by verifying identification. Children sometimes have easy access to their parents' personal identification numbers (PINs), passwords, credit card numbers and e-cash (electronic money), although such access usually does not extend beyond the parents' receipt of their first monthly statement showing gambling debts. In the future, we may see voice recognition, video verification, and thumb print or iris verification. Currently, telephone-betting systems involving horse race tracks have built-in safeguards to reduce access by minors.

David Safavian, a principal of Janus-Merritt Strategies, L.L.C., a Washington, D.C., consulting firm testified as a representative of the Interactive Gaming Council (IGC), which is the trade association for operators and suppliers of interactive wagering systems. Mr. Safavian asserted, "It is in the operators' best interest to screen out minors from the system …." He cited the operators' desire to avoid charge-backs and liability "down the road." He added that, based on his observation of some of the 62 operators with the IGC and the technology available to them, they are "making their best efforts" to avoid taking bets from children. Mr. Safavian contended that by

relying on credit cards and cross checking databases operators can have gamblers verify who they are with a reasonable degree of assurance.

Mr. Safavian noted that the IGC has “called for hard hitting third party governmental regulation of Internet gaming.” He testified: “And let me take a second and say that no one in this [hearing] room, I suspect, believes the current state of play is appropriate or in the best interests of the Internet, the player [or] the gaming industry. Open and unregulated interactive wagering is not a good idea.”

Australia has an official regulatory system in place in five territories for Internet wagering involving horse racing and sports betting. The system purportedly protects consumers and permits taxation. Liechtenstein operates "Inter Lotto," which has a guaranteed weekly jackpot. A “Big Five” accounting firm, PricewaterhouseCoopers, audits the site. Other countries with licensing laws for Internet gambling include Antigua and Barbuda, Austria, Belgium, Cook Islands, Costa Rica, Curacao, Dominica, Dominican Republic, Finland, Germany, Grand Turk, Grenada, Honduras, the territory of Kalmykia in Russia, Mauritius, St. Kitts and Nevis, St. Vincent, South Africa, Trinidad, Turks and Caicos Islands, Vanatu, and Venezuela. Unlike the situation involving child pornography, where there is realistic hope that through strenuous lobbying and enforcement those in favor of a ban may convince the lion’s share of nations to crusade against such material, Internet gambling is an activity gradually being embraced by much of the world.

Of course, the fact that Internet gambling serves a growing public demand cannot be determinative with regard to legalization. After all, New Jersey, like most jurisdictions, continues to enact and enforce laws against narcotics, prostitution, bookmaking and other vices, even though complete eradication has proven impossible due to ongoing public demand. And some governmental efforts at reducing public demand, such as those involving tobacco products, have actually met with success.

JUSTIFICATION FOR PROHIBITION

The justifications for the prohibition of Internet gambling were outlined in the testimony of Assistant Attorney General John Peter Suarez, Director of the New Jersey Division of Gaming Enforcement, and fall into three broad categories:

- **Sovereignty Protection.** Each jurisdiction has its own carefully crafted policy on gambling, which has usually evolved over time, and which theoretically takes into account the moral, legal and economic considerations that will best address the needs and

desires of its population. Internet gambling nullifies this policy by making casino gambling and sports betting available to all citizens with access to a computer. This should not be viewed as analogous to having its citizens travel to another jurisdiction where gambling is legal, but, rather, as the equivalent of having outsiders come in and open casinos or betting parlors within the jurisdiction's borders.

- **Consumer and Public Protection**. Internet gambling involving casino-style games raises numerous consumer and public protection concerns including: the integrity and financial resources of the operators; the fairness of the games and the possibility of tampering by operators or hackers; the availability of effective consumer-dispute resolution procedures; underage gambling; problem gambling; and criminal activity, including the misuse of patrons' financial information, money laundering, etc. Except for the fairness of the games issue – because the outcomes are public knowledge and are presumably beyond the control of the operators – Internet gambling involving sporting events still raises all the other consumer and public protection concerns.

- **Economic Protection**. In jurisdictions that have legalized casinos or sports books, such gambling businesses create jobs, pay taxes and provide other economic benefits. Real gambling businesses, which are closely regulated and generally bear the costs of their own regulation, also participate in programs designed to address the social problems associated with gambling activities. Internet gambling presently competes unfairly with real gambling businesses because it is not locally regulated or taxed. It also creates no local economic benefits, simply siphoning off profits and leaving all resulting social problems to be addressed by others.

Prohibition of Internet gambling could involve federal and/or state activity. Prohibition has been recommended by the National Gambling Impact Study Commission and, in its final report issued in March 2000, by the Public Sector Gaming Study Commission.

EFFECTIVENESS OF PROHIBITION

In most cases, state and federal laws prohibiting various forms of gambling were adopted before the creation of the World Wide Web. Owing to the international nature of the business, such laws have achieved only nominal success in curtailing Internet gambling. Whether tightened prohibitions would have a significant impact on offshore operators and their U.S. customers is not clear. Such operators often are beyond the reach of U.S. laws, and their patrons can effectively mask their activity.

According to the National Association of Attorneys General (NAAG), of which New Jersey is a member, the federal Wire Communications Act of 1961 (Anti-Bookie Act), 18 *U.S.C.* §1084, insufficiently prohibits gambling over the Internet. The NAAG cites six "major deficiencies" in the law:

- It only covers people in the gambling business. It is not a federal crime to make a bet, even if it is illegal for someone else to take it.

- The law clearly prohibits taking wagers on sporting events, but it is unclear whether other forms of gambling, such as lotteries or Internet casinos, are covered.

- It is a crime to send information that aids in the making of wagers, but the law is ambiguous about receiving such information. An Internet gambling operator could claim that its computers were simply passively receiving bets.

- The law is limited to "wire" communications, meaning telephones and telegraphs. An Internet operator could get around the law by using microwave transmitters and home satellite dishes.

- Telephone companies are not criminally liable if an illegal bookie uses a telephone, but the NAAG wants Internet service providers to fall under section 1084. The ISPs would have to keep track of and censor messages sent by their Internet customers.

- The present law does not allow a "prospective remedy" for law enforcement. The NAAG wants Internet gambling operators closed down before they commit crimes.

Thus far, the federal Department of Justice has brought charges against 22 Internet gambling operators for alleged violations of the Wire Communications Act. All the defendants operated their businesses offshore and maintained that they were licensed by foreign governments.

In March 1998, a federal grand jury in New York indicted 22 offshore Internet gambling operators for conspiracy to use telephone lines to handle sports bets online. Some of the operators had U.S. offices, including one who operated his business from Cliffside Park, New Jersey. The operators charged were the most easily targeted: U.S. citizens, some living in the United States at the time of their arrests. Ninety percent of the customers were in the United States. The companies advertised their services via magazines, spam and their own Web sites. Bettors deposited $100 to $500 to open accounts and

then placed bets via computers or toll-free phone numbers.

The office of U.S. Attorney Mary Jo White sent letters to telephone companies directing them to discontinue service to the operators. Of the 22 defendants, 15 entered guilty pleas and six remain fugitives. Only one defendant, the co-owner and operator of an offshore sports book, elected to proceed to trial.

In February 2000, a federal jury convicted the defendant of violating the Wire Act by accepting bets from Americans over the Internet and by telephone. The defendant, who faces up to 19 years in prison, was scheduled for sentencing in May and has indicated that he intends to appeal.

Four states — Louisiana, Illinois, Michigan and South Dakota — have prohibited online betting by statute. The National Gambling Impact Study Commission reported that a number of state attorneys general have initiated court action against Internet gambling owners and operators and have won several permanent injunctions. Some companies have been ordered to dissolve, and their owners have been fined and sanctioned. However, in noting that the impact has been limited, the Commission concluded: “The large majority of Internet gambling sites, along with their owners and operators, are beyond the reach of the state attorneys general.”

Legislation signed on July 17, 1997, made Nevada the first state to explicitly prohibit — and allow — Internet gambling. The Nevada law permits licensed race and sports books, off-track pari-mutuel betting operators and casinos to accept wagers via the Internet. Therefore, it is a state crime for a Nevada resident to make an out-of-state bet over the Internet, but legal under that state’s law for certain Nevada operators to accept wagers from anywhere in the world.

Florida Attorney General Robert A. Butterworth succeeded in persuading Western Union to stop wiring money to 40 offshore sports books. Some customers switched to Federal Express to forward checks to the operators. Florida’s Office of the Attorney General also mailed letters to media throughout the state advising them to “cease and desist” advertising for offshore sports books. This did not foreclose other forms of advertising, such as targeted e-mail, chat rooms and the like.

On January 8, 1998, the Coeur d’Alene tribe initiated a "US Lottery" in approximately three dozen states where lotteries are legal. It ran the lottery through a server located on its reservation in Worley, Idaho. In December 1998, the U.S. District Court in Idaho ordered the tribe to cease operations. The tribe then notified players that it had decided to shut down the enterprise.

Adversaries of illegal Internet gambling have enjoyed some

success attacking the financial transactions necessary to pay off wagers. Some experts contend that about 85 percent of online bettors use credit cards. The card issuers and banks worry about charge-backs, where a player can stop payment on his losing bets. They have considered banning gambling charges because of recent lawsuits by bettors contending they do not have to pay debts incurred from illegal activity. The National Gambling Impact Study Commission mentioned two such cases. The lawsuits have caused some foreign operators to conclude that they must have the money in hand in their countries, via wire transfers or other forms of payment, before they can accept wagers. This reduces the number of customers willing to patronize those operations.

So long as they avoid stepping on U.S. soil, foreign Internet gambling operators may effectively be beyond the reach of any American law. With perfect scramblers coming online, crooked operators will be able to hide anywhere in the world, according to Professor I. Nelson Rose of Whittier Law School. They could post an official licensing seal from Australia and pretend to their customers to be operating legitimately. Under such conditions, authorities could put Internet gambling out of business only by frightening away customers — an endeavor that might be as futile as Prohibition was for the control of liquor consumption.

Although gambling via home computer might violate state laws and may be subject to creative legislation and civil and criminal enforcement actions, only the federal government may have the full panoply of resources to aspire to curtail such activity. Recognizing the difficulties posed by Internet gambling, the NAAG, with the approval of New Jersey among numerous other states, passed a resolution in mid-1998 asking Congress to create a new federal crime part of which would have made it a misdemeanor to make a bet on the Internet. Wisconsin Attorney General James E. Doyle, who co-chaired NAAG’s Internet Working Group, wrote to William A. Bible, Chairman of the National Gambling Impact Study Commission’s Subcommittee on Regulation, Enforcement and the Internet, that “NAAG has taken the unusual position that this activity must be prohibited by federal law, and that State regulation would be ineffective.”

Federal prohibition against bettors would force the federal government to go after gamblers who make wagers from their personal computers at home. The U.S. Department of Justice opposed the idea because it did not want to be in the business of arresting gamblers. Despite the practical difficulties of enforcement, however, the National Gambling Impact Study Commission recommended a federal ban on Internet gambling.

Although the U.S. Senate passed Senator Jon Kyl's (R-AZ) bill, the "Internet Gambling Prohibition Act," the House counterpart, *H.R.* 4427, sponsored by Frank A. LoBiondo (R-NJ) died in the House

Judiciary Committee in October 1998. The bills would have amended the Interstate Wire Act to punish Internet gambling operators and bettors and to require Internet service providers (ISPs) to block out gambling sites. The bills were reintroduced in 1999 (see *S.* 692). They would provide an exception for pari-mutuels, but an amendment offered to the Senate bill by Robert Torricelli (D-NJ) would require permission from a state's racing commission before an interactive wagering provider would be permitted to accept accounts from residents of that state.

The 1999 version of the Kyl Bill (which does not criminalize the act of betting on the Internet) was passed by the United States Senate in November 1999. A companion bill in the House of Representatives (H.R. 3125) was approved by the Judiciary Committee in April 2000. It is not clear at this time whether a federal ban on Internet gambling will ultimately be enacted, what form such a ban will take, or if any ban will be enforceable and effective.

If enacted, the federal bills would provide a mechanism for having interactive computer service providers remove or disable access to offending Internet gambling sites at the request of federal or state law enforcement authorities. This, coupled with other potential legislation against credit card companies and other financial service providers, advertisers, and other businesses which facilitate Internet gambling, could be very effective in limiting the availability of such gambling in New Jersey and the United States.

In any event, a legal prohibition does not need to be 100 percent effective in order to achieve its goals. The prohibition would be effective if it deterred a majority of law-abiding citizens from the undesirable activity. Thus, while determined bettors in a prohibiting jurisdiction may still find ways to gamble on the Internet, most citizens will likely avoid Internet gambling in favor of other, legal methods, at least where such alternative outlets are available and convenient. And most substantial businesses and financial entities — particularly those already involved in legal gaming — will probably shun any industry tainted by the stigma of illegality.

On the other hand, it should be remembered that liquor Prohibition led to the entrenchment of organized crime in America. There is a concern that a large-scale investment of enforcement resources might simply succeed in driving the would-be respectable cyber-gambling operators out of business, leaving the field to scoundrels. If it forced the remaining operators to congregate offshore, prohibition might have the unintended effect of actually increasing the exposure of children and compulsive gamblers to online wagering. Meanwhile, it could create a black market that would enrich offshore companies at the expense of domestic gambling enterprises and the U.S. economy.

JUSTIFICATION FOR REGULATION

Some observers believe that prohibition promotes unlawful activity while regulation diminishes it. Many believe that for the protection of the industry and consumers Internet gambling should be regulated by a federal agency with adequate enforcement powers. The federal District Court in New York recently ruled in a pornography case that it would burden interstate commerce unduly to have 50 different state laws apply to the Internet.

Mainstream gaming providers in the United States, such as legitimate casinos and race tracks, might want to tap into the Internet gambling market, but first a widely accepted regulatory system would have to replace the prohibitive approach now guiding most North American jurisdictions. Otherwise such providers would jeopardize their standing in the legitimate casino and pari-mutuel industries. For the time being, the absence of regulatory oversight in the United States diminishes American consumers' confidence in the integrity of cyber-gambling and keeps demand relatively low. However, Internet gambling businesses expect revenue to grow as they build trust both within and outside regulatory mechanisms.

John E. Shelk, Vice President of Government Affairs for the American Gaming Association (AGA), whose members are the principal casino resort operators in Atlantic City, Las Vegas and elsewhere, testified that self-regulation and voluntary guidelines would not be sufficient. He noted that the minimum age for casino gamblers is 21, but 18-year-olds can obtain credit cards. He added that casinos in New Jersey, Nevada and elsewhere have to abide by strict licensing requirements overseen by independent third parties.

Mr. Shelk pointed out that, putting aside Native-American gaming with its unique legal status, commercial gaming of the type occurring in Atlantic City is legal in just 11 of the 50 states. Sports betting, which Mr. Shelk called "the predominant form of Internet wagering today," is legal in just two states: Nevada and, to a limited degree, Oregon, which links certain lottery games to sports outcomes. Thus, wholesale permitting and regulating of those two forms of gambling alone over the Internet would in itself involve a major acceleration of the official countenancing of gambling activity in America. Most observers acknowledge, however, that a huge volume of such gambling, as well as other varieties, already takes place in the underground economy. Recognizing this "conundrum," Mr. Shelk testified:

> But at the present time, we do have a situation where we have unregulated gaming taking place, and that's what we've always opposed, because we believe the integrity of the game is fundamental to preserving the confidence the customers have in the gaming opportunities that we and others offer.

Given a choice, most consumers will participate in a regulated environment when it competes with an unregulated one, because they want to avoid being victimized by unscrupulous operators. Although a rogue company could always exist beyond any regulatory pale, its customer base would shrink as a regulated industry satisfied consumer demand. The cost of relocating to new Web addresses to avoid regulatory sanctions would function as the ultimate market-driven enforcement mechanism.

Some have suggested that an effective regulatory system would require applicants to prove integrity, suitability, solvency, and willingness to submit to regulations and a code of conduct. Any regulatory scheme should prohibit cyber-gambling by minors and effectively screen them from bettor ranks. It should forbid the extension of excessive credit, mandate exclusion of problem gamblers, protect players' privacy, mandate disclosure of pay outs, require adherence to complaint procedures, and institute licensing of all key employees and owners of at least 5% interest. It also should require submission to audits.

If the Australian Internet-gambling regulatory system proves that the industry can be effectively regulated and that revenue can be generated for the government, a similar model could prove to be acceptable in the United States. Such a system promises to be much more realistic and enforceable than prohibition.

Regulated online gambling regimes may utilize Remote Access Verification Environment (RAVE) technology for non-Internet-based cyber-gambling. RAVE is a product of Bally Gaming and Systems. It restricts dial-up access to subscribers. As a proprietary "intranet," RAVE provides the foundation for an intrastate, closed-loop, subscriber-based gambling system. Security is achieved through sophisticated encryption techniques and the use of smart cards to identify and authenticate users.

David Safavian testified that Alliance Gaming had received approval in February 1999 from the Nevada Gaming Control Board to install an interactive intrastate wagering system. According to Mr. Safavian, a customer would dial into the gaming operator's network from his home computer modem number. The operator would use Caller ID to confirm that the log-on came from the customer's authorized location in a state permitting the operator's forms of gambling.

Several organizations have studied or are studying the complex issues raised by Internet gambling. On November 30, 1999, the National Fraud Center (a fraud and risk management consulting firm and a founding member of the Internet Fraud Council) and Spectrum Gaming Group (a consulting firm founded in 1993 and headquartered in Pennington, New Jersey), began a joint project to help governments and

gaming companies regulate gambling over the Internet. The companies provide regulatory services to governments and work with Internet gaming companies on self-regulating the industry.

In January 1999, a non-partisan group of state legislators formed the National Council of Legislators from Gaming States. Funded by a university research grant, the group and its affiliate members (various state and local government leaders) will focus on the impact of gaming in the areas of state fiscal policies and budgets, law enforcement, state credit ratings, peripheral supporting businesses, educational programs, employment and families.

The Interactive Gaming Council (IGC) was formed in association with the Interactive Services Association in December 1996. The Chair, Susan Schneider, also is CEO and President of The River City Group, LLC, which publishes a subscription-based electronic magazine, *Interactive Gaming News* (www.igamingnews.com). She served as CEO and President of RGT OnLine, Inc. from 1995-98 where she built the *Rolling Good Times Online* consumer publication (www.rgtonline.com). The Council has adopted a "Code of Conduct" for its members and is pursuing the formation of an independent regulatory board for the industry. Representing the IGC at the public hearing, Mr. Safavian emphasized that the IGC “is seeking third party governmental regulation.”

Mr. Safavian listed six recommendations for regulation proposed by the IGC:

1. Enforcement efforts should be focused on the operator, not the bettors.
2. Internet gaming companies should submit to U.S. jurisdiction, via a physical presence or a sizeable bonding requirement, before offering gaming products to U.S. citizens over the Internet.
3. Operators should be licensed. Licensing compliance should involve methods to check the integrity of the operations, screen out problem and under-age gamblers, evaluate the backgrounds of operators and their employees, and collect appropriate taxes.
4. Beyond some federal activity to cope with the international aspects of Internet gambling, enforcement efforts should take place at the state level.
5. In order to ensure parity between cyberspace and the rest of the world, regulation should require operators to respect jurisdictional boundaries, especially as evolving technology permits them to determine the geographic locations of those logging onto their gaming sites.
6. Open and unregulated gaming should not be acceptable.

Pointing out that “marketing is brand name identity,” Mr. Safavian contended that major gaming companies would enter and alter for the better a legalized Internet gambling market. He elaborated:

> I would suspect that we have a number of operators offshore that are merely biding their time until they can sell out, and I'll tell you why. If … I were going to [bet online], and I had a choice between www-dot-no name-dot-com and Caesar's Palace Online-dot-com, I know where I'd put my blackjack bet, and I think others do recognize that.

The North American Gaming Regulators Association (NAGRA) (www.nagra.org) has a Cyberspace Gaming Committee. Frank Miller, Esq., a past President of NAGRA and the former Director of the Washington State Gambling Commission, testified about cyber-gambling on February 4, 1998 before the House Judiciary Committee's Subcommittee on Crime.

EFFECTIVENESS OF REGULATION

Although nearly universal agreement exists regarding what an effective system of Internet gambling regulation should require, it is much less clear that current technology can insure that such requirements are met. Many of the Internet gambling regulatory systems currently extant appear to place significant, if not total, reliance on the integrity of the operators. Although operator integrity is a vital part of any gambling regulatory system, casinos and other real gambling businesses are also subject to continuing and pervasive scrutiny of their activities. Each gambling transaction is monitored, each slot machine program is checked, and each chip is sealed into the machine.

To provide regulators with the same or nearly the same comfort level with regard to Internet gambling, the interactive gaming industry would have to provide cogent and convincing answers to questions such as the following:

1. How will regulators be able to assure themselves that the "prototype" Internet gambling computer program is fair to bettors and complies with all regulatory requirements?

2. How will regulators be able to assure themselves that the computer games that bettors are playing are actually operating in the same way as the "prototype" checked by the regulators?

3. How will regulators be able to assure themselves that the "prototype" is safe from tampering by operators or hackers? How will regulators know whether such tampering has occurred? If tampering does occur, how will regulators deal with it?

4. Is a fair, effective and convenient dispute-resolution procedure available to bettors? How will regulators be able to "recreate" or

audit gambling transactions that have already taken place? How can they assure themselves that the computerized records furnished by the operator have not been altered?

5. How will the Internet gambling operation effectively screen out underage gamblers?

6. How will the Internet gambling operation effectively screen out bettors from jurisdictions that prohibit Internet gambling?

7. How will the Internet gambling operation address the issue of problem gamblers?

8. How will the Internet gambling operation protect the confidentiality of bettors' financial information from internal or external misuse?

9. How will the Internet gambling operation avoid being used as a vehicle for money laundering and other financial crimes?

10. How can the licensing jurisdiction assure itself that it is receiving the amount of tax revenues to which it is entitled?

It may be that existing or evolving technology can provide satisfactory answers to these questions, but such has not yet been demonstrated.

COMPULSIVE CYBER-GAMBLING

Compulsive people often succumb to the lure of gambling and degenerate into insolvency, detachment from family and friends, and despair. Internet gamblers are particularly susceptible to a "cave syndrome" fostered by convenient, varied and isolated gambling 24 hours a day. Easy access to wagering exacerbates compulsive gambling, and there is no greater access than that afforded by the Internet.

The National Council on Problem Gambling, Inc. recognized the multiplying threat of Internet gambling to compulsive gamblers when it established an Internet Committee. The Council on Compulsive Gambling of New Jersey, Inc., which takes no position for or against legal or illegal gambling, is an affiliate of the National Council.

Kevin O'Neill, Deputy Director of the Council on Compulsive Gambling of New Jersey, testified that he developed the following dozen recommendations for Internet gambling organizations that are serious about helping compulsive gamblers:

1. Develop written policies outlining your organization's commitment

to addressing the issue of compulsive gambling.

2. Provide links to compulsive gambling informational, referral and help sites.

3. Participate in industry-sponsored responsible gaming programs like the Interactive Gaming Council's Helping Hand Program.

4. Post national and international compulsive gambling help-line phone numbers.

5. Initiate "loss limits" and cool-down periods for customers.

6. Allow customers who are compulsive gamblers to "self-exclude" themselves.

7. Promote corporate responsibility through financial and programmatic support of both national and international Councils on Compulsive and Problem Gambling.

8. Develop strict policies on the use of credit for gambling purposes.

9. Provide ongoing education for all personnel on compulsive gambling.

10. Encourage all operators to educate the public regarding available software filtering products that can deter underage gambling.

11. Develop strong, highly visible warnings pronouncing "no underage gambling."

12. Support regulations of Internet gambling that clearly address prohibitions of underage gambling and funding for compulsive gambling awareness programs.

David Safavian testified that "the operators are trying to develop a compulsive gambler or problem gambler database that … looks for patterns of compulsion …." He noted that the IGC has a code of conduct binding its members to do all they can to screen out minors and help problem gamblers. He cited a Helping Hand Campaign to encourage the IGC's members to provide links to compulsive gambler help sites.

E-COMMERCE IN ALCOHOLIC BEVERAGES AND TOBACCO

Sales of alcoholic beverages and tobacco over the Internet present different problems for law enforcement than Internet gambling. Whereas the cyber-gambling “product” can be accessed entirely online, alcoholic beverages can be acquired over the Internet only by physical shipment of bulky material, regardless of how the customer pays for it.

The Division of Alcoholic Beverage Control (ABC) in the Department of Law and Public Safety regulates the distribution and sale of alcoholic beverages within the State of New Jersey. Current law in New Jersey, *N.J.S.A.* 33:1-2, and most other states prohibits “mail order sales” of alcoholic beverages to state residents by producers and retailers in other states regardless of whether the orders are transmitted via telephone, mail or the Internet. Such sales bypass state regulatory systems for controlling liquor. They facilitate the delivery of alcoholic beverages to underage persons, the loss of liquor tax revenue and the transfer of alcoholic beverages by unlicensed entities.

A bill pending in Congress, H.R. 2031, would permit the chief law enforcement officer of a state to seek injunctive relief in federal court against those violating state law regulating the importation and transportation of alcoholic beverages. It would permit state enforcement agencies to confront out-of-state shippers with more confidence in their jurisdiction.

A major concern of opponents of online sales of alcohol and tobacco is the potential that these products will fall into the hands of minors on a grand scale. In the case of tobacco, the attorneys general of 13 states, including New Jersey, have taken steps to stop online merchants from selling to children a popular brand of hand-rolled flavored cigarettes from India called bidis (pronounced bee-dees). Whether orders are placed by telephone or via the Internet, minors have been able to buy bidis without being asked their age. Law enforcers and anti-smoking advocates are particularly incensed because the candy or fruit flavoring added to bidis produced for the American market make them appealing to young people, and their high nicotine and tar content make them more harmful than regular cigarettes.

The online tobacco sellers maintain that their sales are legal because a credit card is needed to make a purchase, and only individuals over 18 can obtain a credit card legally. This defense cannot succeed, however, for sales of liquor in those states, such as

New Jersey, requiring purchasers of alcoholic beverages to be at least 21 years old.

In the last six months of 1999, as many as 70 Web sites offering cigarettes for sale at dramatically discounted prices have sprouted. These vendors generally operate either from low-tobacco-tax states or from Native-American reservations, where cigarettes can be bought free of the 34-cents-a-pack federal excise tax. In either case, consumers may avoid general sales, use or cigarette tax obligations to their home jurisdictions.

CHALLENGES FOR LAW ENFORCEMENT

Computer technology offers many advantages to law enforcement. A computer terminal in a patrol car can help an officer who pulls over a car in a remote area to determine whether he is about to confront someone who has just stolen a vehicle. Another example of high technology helping law enforcement is face-recognition software, which was developed by a Jersey City company. In conjunction with closed circuit televisions in public areas, the software is being used in several areas in the United States and the United Kingdom to match faces in the crowd on public streets with photographic databases of known criminals.

Meanwhile, as society’s use of computers for good has expanded, criminals have adapted the technology to unlawful activities. To counter criminal conduct involving computers, law enforcement agencies will have to enhance their high-technology capabilities, including investigative techniques, equipment, training, and personnel recruitment and retention programs. Moreover, the nature and volume of cyber-crime require cooperation among agencies at every level.

More than perhaps any other area computer crime control requires cooperation between the public and private sectors. Businesses must have confidence that reporting computer crimes and cooperating with investigations will have a positive impact on the bottom line. Law enforcement must earn such confidence. It also must take full advantage of the vast expertise available from private sources that have a keen interest in clean e-commerce and the security and integrity of cyberspace.

SPECIAL PROBLEMS OF COMPUTER-RELATED CRIME

In addition to facilitating a host of high-technology crimes, computers can help to organize traditional criminal enterprises. They provide cheap, high quality counterfeits of financial and other

documents. The hard drives of drug traffickers contain financial records and data about shipments and customers, and Internet connections do away with the need for open-air drug markets that can generate complaints from the surrounding neighborhoods. Bookmakers' computers store records of bets and bettors. Prostitution rings track employees and their customers electronically. Highly sophisticated fraud operations have been detailed in computer records. Even detailed plans for the commission of a murder have been recovered from a perpetrator's computer.

The speed, security and anonymity of cyber-payments (i.e. digital currency or e-money) could render obsolete existing techniques to track money obtained illegally, which currently center on monitoring bank transactions. The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) (www.treas.gov/fincen) is working with other nations and the cyber-payments industry to attempt to develop effective measures to prevent and detect financial crime and money laundering. It is predicted that digital currency will be widely available to the public by the year 2002.

Computers give participants in criminal schemes the ability to communicate in secret via encrypted messages, over what public hearing witness John Lucich called "virtual private networks." For example, the Cali Cartel, one of the key Colombia-based narcotics-trafficking groups, has used high-tech encryption to make it difficult for law enforcement officials to trace any telephone communications made by cartel operatives.

Criminals sometimes hold "meetings" with co-conspirators on Internet relay chat (IRC) channels where they can communicate person to person. They can arrange that no one else "sees" what they say to one another. These processes can be used to defeat judicially authorized wiretaps. To discover and hold computer wrongdoers accountable, law enforcement will have to contend with the near perfect anonymity afforded by computer networks and the difficulty of tracing computer communications to their destinations and sources.

Michael T. Geraghty, a member of the team that founded the High Technology Crime and Investigations Support Unit in the New Jersey State Police, now is Network Intrusion Detection Manager for the Corporate Computer and Network Security Division of Lucent Technologies. Mr. Geraghty testified how encryption technology can be a mixed blessing in the fight against computer-related crime:

> As [encryption] becomes easier to use, it's going to be a hindrance in carrying out investigations. However, at the same time, and I know I'm not in the majority on this, I think encryption is probably going to be the answer to a lot of our privacy problems online, a lot of the intrusion problems online. It's going to take away a lot of the crime … if we can have

> strong encryption over the Internet. No longer will you be able to pull my credit card number out of a server if encryption is used properly. So I think on the one hand, it's going to hinder law enforcement from looking at a bad guy's hard drive or a bad guy's communications. On the other hand, I think it's going to protect the public like nothing else can protect the public.

Law enforcement must act quickly in order to preserve evidence of computer-related crime. For example, in tracing those who use computers for criminal activity, law enforcement can seek the computerized records that Internet service providers (ISPs) keep of their customers' account activity. An Internet Protocol (IP) Address identifies each online session during which a particular customer connects to the ISP. It is located in the headers on each Internet communication. The ISP can identify the account used to commit a crime when provided with the proper legal document, the IP Address, and the date, time and time zone of the communication. However, ISPs typically keep their customers' session records only for short periods of time.

Identifying the ISP account used to commit a criminal act is only the beginning of identifying the perpetrator. Online criminals "steal" Internet accounts to direct suspicion away from themselves and toward innocent account holders. In these cases, law enforcement officials have to trace money, deliveries or telephone calls to the criminal.

The public hearing highlighted the need to follow proper procedures when searching for and seizing computer-based evidence. Successful seizure, handling, retrieval and preservation of such information — sometimes called computer forensics — require specialized skills. Since online crime is committed via computer, there are two scenes of the crime: the victim's computer and the criminal's computer. Each may contain evidence or leads that may help to thwart a crime in progress.

John Lucich testified about the need for a topflight computer forensics operation at the state level, complete with highly trained non-law enforcement personnel in support positions. He related that Florida has "one of the most successful state run labs … in the United States." He added:

> [Florida has] developed a system that when a law enforcement officer seizes a piece of equipment, within a couple of hours, they work on that and seize initial information off there for the investigator to often go off and do more investigation. Today, in a lot of other states, including … New Jersey, it's often months before somebody can get access to the initial information off that hard drive. … But they have private individuals, non-law enforcement, that support the law enforcement effort, and in that respect, they are allowed to pay those individuals even more money. But you also tap into expertise that law enforcement

officers may or may not have, and you can get up and running.

In 1994, the U.S. Justice Department's Computer Crime and Intellectual Property Section published federal guidelines for searching and seizing computers. In April 2000, New Jersey's Division of Criminal Justice issued the *New Jersey Computer Evidence Search & Seizure Manual* to guide law enforcement personnel looking for computer and other digital evidence.

Law enforcers must continue to invest in expensive computer hardware capable of scanning huge hard drives and compressing the data to preserve it. They must purchase software that will expand the same data onto CDs that can be presented in court as evidence. They must learn how to penetrate "booby trapped" operating systems designed to delete material before investigators can retrieve it.

As law enforcement agencies adopt more modern technology, they will have to implement sophisticated security measures to safeguard their sensitive information. In April 1999, for example, a computer hacker compromised a police department's investigation into a riot near the campus of Michigan State University. The hacker broke into the East Lansing Police Department's computer through a Web site and reportedly stole confidential information from nearly 200 informants who were helping police catch rioters who smashed windows and burned a police car after MSU's basketball team lost in the NCAA tournament.

Assisted by high technology, criminals have harassed and disrupted police investigations in other ways. For example, a northeastern police department in the midst of a major drug investigation learned from an informant that the targets were intercepting the agency's cellular telephone communications. Computer hackers also have stolen investigators' credit information to disrupt their lives with phony credit charges, bogus liens and the like.

JURISDICTION

Jurisdiction is one of the greatest challenges to state and local enforcement in the Internet age. Oftentimes, the person trying to break into a computer or send pornography to, or lure, a New Jersey child is doing so from another state. Likewise, the information necessary to investigate the case may also be in another state. These two scenarios point up the thorny problems of jurisdiction in a cyber-world without borders.

The dilemma of trying to obtain the information necessary to further an investigation is particularly vexing. Territorial jurisdiction over a criminal episode is addressed in *N.J.S.A.* 2C:1-3, which extends the jurisdiction of the courts of New Jersey over

matters where “conduct which is an element of the offense or the result which is such an element occurs within [New Jersey].” Thus, a person may be held criminally accountable in New Jersey for behavior committed in another state.

The situation is not so clear-cut when it comes to obtaining the evidence of the commission of a crime that exists out-of-state. Many of the largest companies providing access to the Internet are located outside New Jersey. It is the policy of many of those companies that it is necessary to obtain appropriate process from the jurisdiction where the company offices are located before they will disclose requested information. This involves a complicated and time-consuming process of either contacting law enforcement in sister jurisdictions to put together the process necessary to obtain the requested information, or the equally cumbersome process of obtaining interstate subpoenas. Such a requirement is particularly frustrating in that often the requested information involves records of communications that took place between two individuals in New Jersey. However, because the Internet service provider that maintains the records of the New Jersey communications is out-of-state, law enforcement is forced to follow time-consuming procedures to obtain that information. Since computer evidence in general, and the records relating to electronic communications in particular, are volatile and routinely destroyed in the ordinary course of business, the delays encountered in obtaining the process that the Internet service provider will honor can result in the loss of crucial evidence. Any solution to this issue is complicated because of the intricate jurisdictional relationships between and among the states and the federal government that date back to the mid-nineteenth century.

California recently enacted a law to address the issue of jurisdiction in two related ways. Section 2105(a) of the California Corporation Code requires foreign corporations doing business in California to accept warrants for information and records of electronic communication services or remote computing services located outside the state. Section 1524.2 of the California Penal Code provides that a foreign corporation shall produce the requested records within five days of service (*CAL PENAL* § 1524.2(b)(1)). A California corporation shall treat all warrants for information from providers of electronic communications services or remote computing services to the public from states other than California as if they were issued in California (*CAL PENAL* §1524.2(c)). The effect of these statutes is to require any corporation doing business in California to provide records relating to the provision of electronic communication services and remote computing services, as they are defined in 18 *U.S.C.* § 2701 *et seq.*, even if the corporation’s offices and the information sought are out-of-state. In addition, the legislation substantially assists law enforcement from other states by making California corporations subject to warrants from other states as if California courts had issued them. California has unilaterally

established a system similar to an interstate compact, thereby overcoming some of the jurisdictional hurdles that state and local law enforcement encounter.

If a similar statutory regimen were enacted in New Jersey, it would dramatically reduce the time it takes to obtain records and other information from electronic communication services and remote computing services such as Internet service providers. This type of legislation also would subject foreign corporations, which do substantial business in New Jersey, to the jurisdiction of this state's law enforcement for service of process to obtain crucial information in the investigation of Internet-based crimes.

SPECIALIZED COMPUTER CRIME UNITS WORKING TOGETHER

No single law enforcement agency can muster sufficient gadgetry and know-how to address computer crime successfully in isolation. With enhanced cooperation among large and small agencies, however, the same technology that assists criminals can provide boundless opportunities for even a small police department to take advantage of almost limitless resources. For example, with a remote terminal in a patrol car, a small-town police officer can obtain immediate help from huge databases of motor vehicle, fingerprint, fugitive and criminal record information.

At a meeting of the National Association of Attorneys General in January 2000, U.S. Attorney General Janet Reno called for a LawNet organization of federal, state, local and even international agencies to control Internet lawbreakers. As envisioned, teams of highly skilled computer crime prosecutors and investigators from various agencies would have access to regional computer forensics laboratories and other shared technology. Also, a new interstate compact would help ensure enforcement of out-of-state subpoenas and warrants stemming from Internet investigations. Thus, a significant role of the proposed LawNet would be to address questions of jurisdiction.

New York City Police Department Detective Sergeant James Doyle testified about several states and cities that have dedicated specialized units to computer crime control. They include Massachusetts; Sacramento and Santa Clara in California; Chicago; Illinois State Police; New York City; New York State Police; New Jersey State Police; Florida; Delaware; and Maryland State Police. However, most of these units have modest resources. John Lucich testified that "some of these units on a statewide level have two people …." He noted, "Pennsylvania, which is a very large state, has now three people in that unit run by a corporal."

Sergeant Doyle testified that his unit has nine law enforcers,

including six investigators, two sergeants and one lieutenant for "the whole City of New York." He said his caseload "has doubled every year." He bemoaned, "[A]nyone who has a computer crime lab at this point, the minimum is about six months to get something looked at, unless there's some sort of compelling reason it has to get done right away – for grand jury or something of that nature." Sergeant Doyle added that the State of New York's unit "has four investigators right now." Abigail Abraham, who heads the Computer Crimes Investigation Bureau of the Illinois State Police, testified that she had five people working for her, with a promise of nine more.

No agency in New Jersey keeps statistics on how many municipal police departments have officers trained to investigate computer crimes. Even if law enforcement agencies all had substantial resources, they would still have to coordinate with one another to an unprecedented degree in order to combat computer crime successfully. The boundless Internet, complexity of computer crime detection methods and potential to tread unwittingly on each other's cases all cry out for extensive collaboration among a multitude of agencies with overlapping jurisdiction. Such cooperation demands frequent and rapid communication secured by a variety of authentication levels and encryption devices.

Recognizing the extreme importance of sharing expertise and coordinating efforts to combat computer crime, top former and current law enforcement officials and high technology security personnel have created helpful professional organizations. New Jersey-based professionals are in the forefront of such activity. The High-Tech Crime Network, for example (www.htcn.org), is located in West Caldwell, New Jersey. Its mission, since its founding in 1991, has been "to unite the law enforcement and corporate sector in the fight against high-tech related crimes."

As noted above, the High-Tech Crime Network's Founder and President, John Lucich, a former top computer crime investigator for New Jersey's Division of Criminal Justice, testified at the public hearing. Currently, Mr. Lucich is President of Secure Data Technologies Corp. of Fairfield, New Jersey. The Chairman and CEO of Secure Data Technologies, Thomas Welch, who also testified at the public hearing, is a member of the Editorial Advisory Board of *The Journal of Computer Crime Investigation & Forensics*, which is published quarterly by the High-Tech Crime Network.

Another witness at the public hearing, Michael Geraghty, is the immediate Past President of the Northeast Chapter of the High Technology Crime Investigation Association(www.ne-htcia.org/index.htm). Currently Network Intrusion Detection Manager for a division of Lucent Technologies, Mr. Geraghty helped to form and develop the High Technology Crime and Investigations Support Unit of the New Jersey State Police. Public hearing witness Detective Sergeant

James Doyle – also a former President of the Northeast Chapter of the High Technology Crime Investigation Association and its current First Vice President – supervises the Computer Investigations and Technology Unit of the New York City Police Department. Public hearing witness Abigail Abraham, the head of the Computer Crimes Investigation Bureau of the Illinois State Police, founded and was the first President of the Midwest Chapter of the High Technology Crime Investigation Association. These and similar organizations around the country provide significant assistance to law enforcement personnel trying to cope with the complexity of computer crime-related investigations. See the *Law Enforcement Internet Intelligence Report* at www.lawintelrpt.com.

Computer crime control units have an important obligation to reach out to students, parents, small businesses and the broader law enforcement community to let them know how to recognize, prevent and report computer-related crime. They should maintain Web sites to educate the public about current computer crime threats and to receive online complaints.

John Lucich testified about the utility of the task force approach in controlling high-technology crime. He said he would like to see a High-Tech Crimes Prosecutor similar to the Environmental Prosecutor that once existed in New Jersey or the Insurance Fraud Prosecutor that currently exists here. Such an office would coordinate the activities of state and county officials, according to Mr. Lucich.

Michael Geraghty testified that one factor hampers New Jersey agencies' effective participation in task forces with federal agencies and other states. Just to obtain subscriber information based on an e-mail address provided by an ISP, New Jersey law enforcement authorities must prepare affidavits for a communications data warrant that can be issued solely by a limited number of specially designated judges. A subpoena, which is satisfactory in other states or in federal investigations, is not enough for New Jersey law enforcers. If federal or non-New Jersey state or local authorities obtain information via procedures not tolerated by New Jersey's Constitution, as interpreted by the New Jersey Supreme Court, the sharing of that information with New Jersey authorities may jeopardize a prosecution in New Jersey state court. This may prove to be an obstacle to effective inter-jurisdictional task force activity in some circumstances.

Mr. Geraghty added, "[T]he time that it takes to get a communications data warrant can make or break your case in a lot of these Internet cases, and that's because Internet service providers aren't bound by any law to maintain records or maintain logs for a period of time." He concluded, "[T]he more time you take, the less chance those logs or those records are going to be there …."

New Jersey has concentrated much of its computer crime fighting efforts in two specialized units: the High Technology Crime and Investigations Support Unit in the Division of State Police and the Computer Analysis and Technology Unit in the Division of Criminal Justice (DCJ). These two units coordinate their activities to avoid duplication of effort. Along with federal, county and municipal law enforcement representatives, they comprise the Statewide Computer Crime Task Force, created in December 1999 and growing out of the cooperation established during the Melissa virus investigation. The Task Force intends to combat computer crime proactively, but lack of resources limits its ability to do so more than occasionally.

COMPUTER ANALYSIS AND TECHNOLOGY UNIT (CATU)

With just two deputy attorneys general and three investigators, the CATU, which was established in 1998, performs four crucial functions in the effort to control high technology crime:

- Technical assistance in the search and seizure of computer and other digital evidence by DCJ, other state agencies, and county and local law enforcement organizations.
- Legal advice and assistance to the above organizations.
- Forensic analysis of evidence.
- Investigation and prosecution of complex and high-priority computer and Internet crimes.

The CATU’s workload is immense. It has seized entire computer networks in aid of insurance fraud investigations.

HIGH TECHNOLOGY CRIME AND INVESTIGATIONS SUPPORT UNIT (HTC&ISU)

Begun as a pilot program with a detective, a supervisor and two civilian employees in December 1995, the HTC&ISU currently enjoys a favorable reputation in law enforcement circles as one of the most capable computer crime control units in the country. Now numbering nine sworn law enforcement personnel and two civilian employees, the Unit is one of the largest state organizations dedicated to fighting computer crime. Initially tasked to install, maintain and support all of the Criminal Investigations Section’s personal computers, the Unit now devotes the vast majority of its resources to investigating or assisting in the investigation of a broad range of computer-related crimes, including forensic examination of computerized evidence. The number of matters it has handled has roughly doubled every year since 1996.

The HTC&ISU provides training to any law enforcement agency, as well as civic, business and educational organizations. It has been overwhelmed by requests for training and hands-on presentations. The number of such requests increased 50 percent from 1998 to 1999 and came from agencies as far away as Michigan and New England.

Personnel from the HTC&ISU have helped prosecutors' offices in Burlington, Ocean, Salem, Somerset, Bergen and Monmouth counties to establish their own computer crime investigation units. They also assisted state police in Delaware, Maryland, Michigan and New Hampshire with the creation of computer crime control units.

The State Police Web site is being updated to provide information regarding computer safety and ethics, as well as the proper methods to report computer crimes. This will implement the Department of Law and Public Safety's responsibilities under the High Technology Crimes and Interactive Computer Services Protection Act, which took effect on May 1, 1999. The Unit also will help the Department of Education and school boards to fulfill their obligations under the Act to safeguard students using the Internet at school.

The HTC&ISU plans to provide computer security awareness training for businesses. Not only would this help to prevent computer-related crime, it would encourage victimized businesses to involve law enforcement in the capture of perpetrators.

The HTC&ISU also plans to establish a database of information about individuals using computers for criminal activity. The database could serve as a central repository serving the entire state.

With its resources in constant demand, the HTC&ISU can only occasionally engage in proactive investigations in which Unit personnel, working undercover, search the Internet for those bent on criminal activity. If more civilian personnel could be hired to perform technical forensic assignments, it would free more of the Unit's sworn law enforcement personnel for proactive work, including participation in task forces with other agencies.

Budget limitations and purchasing practices limit the Unit's ability to expeditiously obtain state-of-the-art hardware and software. Although the private sector has offered to donate equipment, software and services that would add to the Unit's effectiveness, ethical concerns restrict the Unit to the State's resources and processes.

Currently, the HTC&ISU is in the last year of a three-year Edward Byrne Memorial Grant providing $100,000 per year for three years, with $75,000 coming from the federal government and $25,000 coming from the State each year. The money is used to update equipment and training

and was recently used to purchase computer furniture for expanded quarters to house the Unit at State Police Headquarters.

TRAINING

It is crucial that a core group of investigators and prosecutors receives enough training to handle computer-related cases properly. In addition, it is vital that civil attorneys who investigate and prosecute non-criminal violations of law relating to computers and the Internet receive similar training. In New Jersey, the divisions of Criminal Justice and State Police have begun to implement specialized training programs for law enforcement. The Statewide Computer Crime Task Force is in the process of designing and implementing a training program for deputy attorneys general and assistant prosecutors who must investigate and prosecute computer-related crimes.

Although training is essential to long-term success in controlling computer-related crime, conducting it can distract the current small group of experts from what Mr. Geraghty described as “their normal everyday functions of solving crimes in their own jurisdiction.” That is why a “train-the-trainers” activity, once fully implemented, eventually will free the top experts to devote the bulk of their time to crime fighting activity.

The State Police’s High Technology Crime and Investigations Support Unit (HTC&ISU) provides training to local law enforcement officers and makes informational presentations to civic, business and educational groups. While no agency in New Jersey keeps statistics on how many municipal police departments have officers trained to investigate computer crimes, the number of requests for such training increased 50 percent from 1998 to 1999.

From November 1997 to June 1998, a Deputy Attorney General in the Division of Criminal Justice (DCJ) was assigned to the U.S. Department of Justice’s Computer Crime and Intellectual Property Section under a fellowship sponsored by the National Association of Attorneys General. The first of its kind, the fellowship gave this Deputy Attorney General, who in 1998 became Chief of DCJ’s Computer Analysis and Technology Unit, the opportunity to study all aspects of high technology crime and to share his expertise with training programs throughout the country. The Division currently is working with other state and federal agencies, including the U.S. Department of Justice, to develop high technology crime training programs for state and local police and prosecutors in New Jersey and elsewhere.

In late 1999, DCJ established the Computer and Telecommunications Coordinators (CTC) program in which select assistant prosecutors representing New Jersey’s 21 county prosecutors’ offices meet

bimonthly with DCJ deputy attorneys general to address the impact of emerging technologies on law enforcement in New Jersey. The CTC program is designed to elicit input from experienced prosecutors in order to identify new computer and telecommunication issues and attempt to standardize practices for dealing with them. The representatives then pass on what they have learned to their colleagues and make recommendations for more formal training.

The High Technology Crimes and Interactive Computer Services Protection Act, effective May 1, 1999, appropriated $150,000 to New Jersey's Department of Law and Public Safety to prepare for Internet distribution guidelines and recommendations on computer ethics, proper methods for reporting high technology crimes, safe computing practices for children and their families, and methods to filter, screen or block the receipt of objectionable material on interactive computer services. In addition, the Department is designing a continuing educational program to inform law enforcement, educational, civic and business groups about the emerging issues of high technology crimes perpetrated through the use of computers.

In recent years, helpful computer crime training has been available to law enforcement from organizations such as the National White Collar Crime Center (NW3C), SEARCH Group, Inc. (the National Consortium for Justice, Information and Statistics), the Federal Law Enforcement Training Center, and the International Association of Computer Investigation Specialists (IACIS). The NW3C offers a collection of Internet resource Web sites at www.cybercrime.org. The IACIS, located at www.cops.org, offers a certification program for computer examiners. The Computer Forensics Certified Examiner (CFCE) designation is awarded to law enforcement personnel who complete the IACIS training and off-site test problems.

Surveys taken in 1997 and 1998 at focus group sessions sponsored by the Infotech Training Working Group (ITWG), which was organized by the U.S. Justice Department's Computer Crime and Intellectual Property Section (CCIPS) in October 1996, revealed that awareness of cyber-crime remains low. There is a greater demand for training than there is training available.

To properly address the growing need for training to cope with high-technology crime, the ITWG evolved in April 1998 into the National Cybercrime Training Partnership (NCTP) (www.nctp.org or www.cybercrime.org), headquartered in Fairmont, West Virginia. Created by state, local and federal law enforcement agencies in April 1998, the NCTP's primary mission is to train computer crime investigators and prosecutors. It also helps to equip them and to coordinate their efforts to curb crime in cyberspace. The NCTP is open to any law enforcement organization whose mandate includes electronic crime investigation, prosecution or training. The New Jersey Division of Criminal Justice is a partner agency.

The NCTP is conducting a comprehensive assessment of the needs of state and local law enforcement for coping with electronic crime. In addition, it distributes a 3-part training video and accompanying manual, *Cyber Crime Fighting*, to law enforcement personnel.

The U.S. Department of Justice, through the CCIPS, chairs the NCTP. The National White Collar Crime Center provides full-time staffers, including instructors, curriculum development specialists and researchers. In addition to law enforcement agencies, the NCTP includes technology research institutions, regulatory agencies whose functions affect electronic crime, and law enforcement professional, training and research organizations. A Vision and Policy Committee has nine members representing key areas or initiatives.

In addition to training, the NCTP is creating and maintaining a clearinghouse to provide points of contact to all law enforcement agencies for technical, legal and policy issues. It is also developing a Secure Collaborative Communications Network (SCCN) that will provide a common platform and protocol among law enforcement agencies at all levels. Moreover, it provides sources of expert guidance to investigators. Lastly, the NCTP is supporting research and development of cyber-tools for law enforcement through its partner agencies.

New Jersey's Division of Criminal Justice (DCJ) is developing training to supplement the *New Jersey Computer Evidence Search & Seizure Manual,* issued in April 2000. In addition, DCJ will participate in the Judiciary's annual Wiretap and Communications Wiretap Data Conference to help judges prepare to review applications for electronic surveillance of digital communications. County police academies and prosecutors' offices have begun to offer introductory computer crime courses to municipal police and county investigators.

Addressing some of the concerns raised in testimony at the public hearing, recent amendments to the New Jersey Wiretapping and Electronic Surveillance Control Act, *N.J.S.A.* 2A:156A-1 *et seq.*, permit better preservation of and quicker access to the records, including subscriber information, necessary to investigate Internet crime. New Jersey's electronic surveillance law now also conforms more closely to federal law. Thus, the changes enable a more rapid reaction to the threat of Internet crime and better coordination between New Jersey law enforcers and their counterparts in the federal government and other states.

RETENTION OF KEY PERSONNEL

Even where law enforcement personnel have been properly trained and equipped, there is no clear career path to effectively utilize the

experienced officer or prosecutor's skills. Two of the witnesses on the law enforcement panel testifying at the public hearing, Michael Geraghty and John Lucich, cut short their law enforcement careers after a few years to pursue high paying, computer security-related jobs in the private sector. Although they found much that was satisfying about their law enforcement service, they cited "bureaucratic nightmares," budget restrictions and lack of appreciation of the need for hard-won computer skills as important reasons for the high turnover among qualified computer crime experts in New Jersey and elsewhere.

Ms. Abraham testified that, by not permitting salaries beyond what an investigator's rank within a larger organization allows, the government's pay structure fails to keep pace with the private sector. She maintained, however, that there are "certain ways in which we can make the [public] employees' lives much better," helping them to cope with frustrations in government. She cited payment of tuition at schools and seminars for specialized training and greater allowance of out-of-state travel for training and coordination with other agencies as prime examples.

According to Ms. Abraham, computer crime units need enough people to have someone to fill in when other personnel pursue specialized computer training or report for training, such as firearm re-qualification, needed to maintain their status within the larger law enforcement organization. She maintained that sufficient personnel help to overcome the problem of turnover when certain members of a specialized computer crime unit pursue opportunities within the larger organization or the private sector. She elaborated that her unit benefited from having a certain number of civilian employees, who tend to serve for lengthy periods and provide continuity. She viewed the higher turnover rate of sworn law enforcement personnel as a normal consequence of career advancement. She indicated that such turnover would not threaten a computer crime unit's effectiveness so long as sufficient training were available to replacement personnel and there were some overlap with departing officers to ensure a smooth transition. She noted that officers promoted out of the specialized unit "cross-pollinate" the larger department with sensitivity to computer issues and become the "enlightened managers that we need at another level."

Mr. Geraghty testified that builders of units dedicated to computer crime control have to "start looking outside the box." He said they have to bring some civilian experts into the State Police and other law enforcement agencies. However, he cautioned that such computer security personnel would require a pay scale comparable to that offered by the private sector.

RECOMMENDATIONS

New Jersey has taken significant steps over the years to ensure that its laws give enforcement agencies the power to combat computer crime. These laws also provide recourse for the victims of cyberspace wrongdoing. In addition, although the State has taken steps to inform the public and schoolchildren of online dangers, more remains to be done.

This state also has established a framework of computer crime-fighting units. Their personnel are conscientious and adept but overwhelmed with booming workloads. The insufficiency of state resources devoted to countering high-tech crime will become more and more conspicuous as society plunges headlong into the computer age.

State and local governments earnestly should devote more personnel, training and equipment to controlling and preventing computer crime. They need to increase computer literacy within the law enforcement community. They also need to work more closely with federal agencies and private organizations to seek out and neutralize online predators, intruders and defrauders before their numbers balloon to unmanageable levels. Lastly, they must increase outreach to the community to promote confidence that law enforcement can help individuals and businesses respond appropriately to computer-related crime. These and other objectives would be advanced by implementing the following recommendations.

STRENGTHEN NEW JERSEY'S COMPUTER AND TECHNOLOGY CRIME LAWS

New Jersey's computer crime law, *N.J.S.A.* 2C:20-23 through 34, was enacted in 1984 and should be revised to deal with computer-related crime in a succinct but comprehensive statutory scheme. Amendments should recognize technological changes, including the establishment of the Internet, occurring over the last 16 years and in the future. Sections recommended for revision appear in italics below (bracketed material removed and underlined material added).

- *N.J.S.A.* 2C:20-23 should be amended to revise the definition of "computer" to be consistent with the federal computer crime statute and the definition of "data" to address the issue of data stored on media that are not within the computer, such as removable disks and external disk drives. The section also should be amended to include definitions of "Internet" and "personal identifying information."

  2C:20-23. Definitions
  As used in this act:

a. "Access" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, [or] computer network, or computer storage medium.

b. "Computer" means an electronic, magnetic, optical, electrochemical or other high speed data processing device or another similar device capable of executing a computer program, including arithmetic, logic, memory, data storage or input-output operations[, by the manipulation of electronic or magnetic impulses] and includes all computer equipment connected to such a device, [in a] computer system or computer network, but shall not include an automated typewriter or typesetter or a portable, hand held calculator.

c. "Computer equipment" means any equipment or devices, including all input, output, processing, storage, software, or communications facilities, intended to interface with the computer.

d. "Computer network" means the interconnection of communication lines, including microwave or other means of electronic communication, with a computer through remote terminals, or a complex consisting of two or more interconnected computers, and shall include the Internet.

e. "Computer program" means a series of instructions or statements executable on a computer, which directs the computer system in a manner to produce a desired result.

f. "Computer software" means a set of computer programs, data, procedures, and associated documentation concerned with the operation of a computer system.

g. "Computer system" means a set of interconnected computer equipment intended to operate as a cohesive system.

h. "Data" means information, facts, concepts, or instructions [prepared for use] contained in a computer, computer system, computer storage medium, or computer network. It shall also include, but not be limited to, any alphanumeric, hexadecimal or binary code.

i. "Data base" means a collection of data.

j. "Financial instrument" includes but is not limited to a check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security and any computer representation of these items.

k. "Services" includes but is not limited to the use of a computer system, computer network, computer programs, data prepared for computer use and data contained within a computer system or computer network.

l. "Personal identifying information" shall have the meaning set forth in subsection a. of section 1 of P.L.1999, c. 117 (N.J.S. 2C:21-17a.), and shall also include passwords and other codes that permit access to a computer, data, data base, computer program, computer software, computer equipment, computer system, computer

network or computer storage medium, where access is intended to be secure, restricted or limited.

m. "Internet" means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

- *N.J.S.A.* 2C:20-24 should be amended to give the law the ability to account for the full expense of the harm or loss caused by an offense. The law should include the cost of repairing or remedying the harm done by an unlawful act and the cost of generating or obtaining and storing data as components of the total value.

2C:20-24. Value of property or services

For the purposes of this act, the value of any property or services, including the use of computer time, shall be their fair market value, if it is determined that a willing buyer and willing seller exist. Value shall include the cost of repair or remediation of any damage caused by an unlawful act and the gross revenue from any lost business opportunity caused by the unlawful act. The value of lost business opportunity may be determined by comparison to gross revenue generated prior to the unlawful act that resulted in the lost business opportunity. [Alternatively, value] Value shall include but not be limited to the cost of generating or obtaining data and storing it within a computer or computer system.

- *N.J.S.A.* 2C:20-25 should be amended to provide that almost all conduct that comprises computer crime falls within that section. The section should include reference to computers, computer systems, computer networks, data, databases, computer programs and computer software. The offensive conduct should be segregated into a series of steps of types of behavior ranging from unlawful access to damaging or destroying computers. The statute should provide for gradation of the offense taking into account the degree of damage caused by the conduct. Also, the statute should make clear that the conduct should be parsed so that a court would be required to impose a separate sentence upon a violation for each type of conduct.

2C:20-25. Computer-related theft; unlawful access; damage

A person is guilty of computer criminal activity [theft] if he purposely or knowingly and without authorization, or in excess of authorization:

a. [Alters, damages, takes or destroys] Accesses any data, data base, computer program, computer software, [or] computer equipment [existing internally or externally to a computer], computer, computer system or computer network;

b. Alters, damages[, takes] or destroys a computer, computer system, [or] computer network, data, data base, computer program, or computer software;

c. Accesses or attempts to access any computer, computer system or computer network, data, data base, computer program, or computer software for the purpose of executing a scheme to defraud, or to obtain services, property, personal identifying information, or money, from the owner of a computer or any third party; [or]

d. [Alters, tampers with, obtains, intercepts, damages or destroys a financial instrument] Obtains, takes, copies or uses any data, data base, computer program, computer software, personal identifying information, or other information stored in a computer or computer storage medium; or

e. Accesses any computer, computer system, computer network, data, data base, computer program, computer software, or computer equipment and recklessly alters, damages or destroys a computer, computer system, computer network, data, data base, computer program, or computer software.

A violation of subsection a. is a disorderly persons offense. A violation of subsection b. is a crime of third degree, except that it is a crime of the second degree if the value of the damage exceeds $75,000. A violation of subsection c. is a crime of the third degree, except that it is a crime of the second degree if the value of the services, property, personal identifying information, or money obtained or sought to be obtained exceeds $75,000. A violation of subsection d. is a crime of the fourth degree, except that (1) it is a crime of the third degree if the data, data base, computer program, computer software, or information has a value of $500 or more, or it is or contains personal identifying information, medical diagnoses or treatments, or governmental records or other information that is protected from disclosure by law or rule of court, and (2) it is a crime of the second degree if the data, data base, computer program, computer software, or information has a value of $75,000 or more. A violation of subsection e. is a crime of the fourth degree, except that is a crime of the third degree if the value of the damage is $75,000 or more. A violation of this section is a crime of the second degree if the offense results in a substantial interruption or impairment of public communication, transportation, supply of water, gas or power, or other public service.

A violation of any subsection of this section shall be a distinct offense from a violation of any other subsection of this section, and a conviction for a violation of any subsection of this section shall not merge with a conviction for a violation of any other subsection of this section or section 10 of P.L.1984, c. 184 (N.J.S. 2C:20-31), or for conspiring or attempting to violate any subsection of this section or section 10 of P.L.1984, c. 184 (N.J.S. 2C:20-31), and a separate sentence shall be imposed for each such conviction.

- *N.J.S.A.* 2C:20-26 through 30 and *N.J.S.A.* 2C:20-32 should be

repealed as the provisions of those sections would be incorporated into the revised *N.J.S.A.* 2C:20-25.

- Amendments to *N.J.S.A.* 2C:20-31 and *N.J.S.A.* 2C:20-33 should be made so those sections reflect the amendments to the computer crime statutes.

2C:20-31. Disclosure of data from wrongful access[; no assessable damage; degree of crime]

A person is guilty of a crime of the third degree if he purposely and without authorization, or in excess of authorization, accesses a computer, computer system, computer network, data, data base, computer program, computer software, or computer equipment [or any of its parts] and directly or indirectly knowingly or recklessly discloses or causes to be disclosed data, data base, computer software, [or] computer programs[,] or personal identifying information [where the accessing and disclosing cannot be assessed a monetary value or loss].

2C:20-33. [Copy or alteration of program or software with value of $1,000 or less] Affirmative defense

[The copying or altering of a computer program or computer software shall not constitute theft for the purposes of chapters 20 and 21 of Title 2C of the New Jersey Statutes or any offense under this act if the computer program or computer software is of a retail value of $1,000.00 or less and is not copied for resale.] It shall be an affirmative defense to a prosecution pursuant to subsection d. of section 4 of P.L.1984, c. 184 (N.J.S. 2C:20-25) that the actor obtained, copied or accessed a computer program or computer software solely for personal use, that the program or software had a retail value of less than $1000 and that the defendant did not disseminate or disclose the program or software to any other person. It shall be the burden of the defendant to prove by clear and convincing evidence this affirmative defense.

INCREASE, TRAIN AND COORDINATE LAW ENFORCEMENT RESOURCES

- Training for the Computer Analysis and Technology Unit (CATU) in the Division of Criminal Justice and the High Technology Crime and Investigations Support Unit (HTC&ISU) in the Division of State Police should be maintained at levels that ensure that these units keep stride with developments in and increased use of technology. As computer related-crimes increase, resources allocated to these units should similarly increase in order to permit the continued efficient operation of investigative and prosecutorial functions.

- In addition to law enforcement personnel, it is critical that

investigators and attorneys who enforce civil laws that are used to combat illicit online conduct (such as the Consumer Fraud Act and the Law Against Discrimination) receive training in order to remain current with technological developments and investigative and litigation techniques related to computer evidence. Therefore, ongoing training of employees of the Division of Consumer Affairs, Division of Law and Division of Civil Rights should remain a priority. Further, periodic reviews of staff and equipment levels should be conducted and those levels adjusted as computer-related cases increase.

- The Department of Personnel, coordinating closely with the Statewide Computer Crime Task Force, should explore ways to compensate key computer crime enforcement personnel to allow the State to be competitive with private industry.

- Each prosecutor's office should be encouraged to consider establishing a specialized unit dedicated to computer-related crime or forensics, such as the High-Tech Crimes Unit in the Union County Prosecutor's Office. Assisted by the Statewide Computer Crime Task Force, police departments should assess whether they also could benefit from establishing such units. At a minimum, every prosecutor's office and police department should send primary and back-up personnel to computer crime and forensics training and give them responsibility for such matters within the office or department.

- Computer crime and forensics curricula should be developed for a complete "train-the-trainers" program for investigators, police, deputy attorneys general and assistant prosecutors who investigate and prosecute computer-related crime. Training available from federal agencies and private organizations should be incorporated into the program. Study of the Division of Criminal Justice's recently issued *New Jersey Computer Evidence Search & Seizure Manual* should be integrated with the training.

- The Statewide Computer Crime Task Force should continue to help to coordinate computer crime control activity among federal, state, county and municipal participants. All agencies with dedicated computer crime control units or personnel should participate at some level. The task force should promote and coordinate effective security measures for law enforcement computer networks and electronic communication throughout New Jersey.

- Law enforcement agencies should encourage their computer crime control staff to become members of the High-Tech Crime Network, the Northeast Chapter of the High Technology Crime Investigation Association or comparable organizations by subsidizing the cost of membership and providing work time to participate in organization

events.

INCREASE PREVENTION AND EDUCATION

- Adults need to develop “street smarts” about the information superhighway in order to protect themselves and their children from computer criminals. Therefore, all school district and community college adult and extension education programs should offer instruction on computer crime recognition and prevention. Four-year colleges and universities should build into their curricula components that alert students about online dangers.

- All public libraries should have at least one Internet access terminal that uses software to screen out offensive material and prevent children from providing personal information over the Internet. Children’s library access to the Internet should be limited to such terminals unless they have parental consent to use unrestricted terminals. Terminals with unrestricted Internet access and reserved for adults should be arranged so that only the user can observe the screen.

- All public schools should determine if there is a need to install monitoring or tracking software on their Internet-connected computers and periodically review student use to detect behavior that warrants counseling.

- All public school teachers whose courses involve student use of the Internet should receive training in the instruction of Internet safety and the application of critical thinking skills to online information. Public school teachers can use the resources of the Educational Technology Training Centers (ETTCs), that include Internet safety training in each training session that addresses Internet activities, and the Commission on Holocaust Education, which works with the ETTCs to offer special training sessions that incorporate topics such as Internet safety and false information about the Holocaust.

- Even though 95 percent of the schools in New Jersey already have an acceptable use policy, it is crucial that every public school district should adopt and fully implement acceptable use policies for filtered and unfiltered stations on their networks. Model acceptable use policies are available on the Department of Education Web site (www.state.nj.us/njded/techno/htcrime/aup.htm).

- The Department of Education (DOE) should ensure that all public school districts fully implement the High Technology Crimes and Interactive Computer Services Protection Act, which took effect on May 1, 1999. The DOE addresses the requirements of the law through

a variety of means, including a special Web site located at www.state.nj.us/njded/techno/htcrime. The Web site offers information about where guidelines and curriculum material on the ethical use of computers, Internet safety, evaluating Web sites and filtering information may be accessed. The Web site is constantly evolving to meet the needs of schools on the potential risks and dangers related to interactive computer services.

- Consideration should be given to providing additional resources to the Commission on Holocaust Education so that it can study the extent of false and misleading information about the Holocaust on the Internet. Then, the Commission should present its findings about the harmful effects of such information to the Department of Law and Public Safety, the Department of Education and local school districts for incorporation into Internet safety warnings and curricula.

- The Department of Law and Public Safety should issue safe computing guidelines on a Web site and publicize its availability. This would implement a key responsibility given to the Department by the High Technology Crimes and Interactive Computer Services Protection Act.

- Internet service providers should be encouraged to prepare carefully, and to enforce strictly, terms of service agreements with their customers in order to bar material containing expressions of hate, indulging in child pornography or exploitation, touting get-rich-quick schemes, or encouraging other offensive activity. Customers should patronize only those ISPs that can demonstrate a significant track record of excluding such offensive content.

ACCESS TO ELECTRONIC RECORDS OF INTERNET USE

- Internet service providers should be required to maintain their customers' session records so that law enforcement authorities can make properly authorized inquiries concerning online criminal activity or wrongdoing. The exact period for mandatory retention should be determined by the technical capability to store such records and the needs of law enforcement, as determined by experience with previous investigations.

- State law should be reviewed to determine whether a new law is needed in order to provide the state Attorney General additional authority to issue administrative subpoenas for computer records.

- New Jersey should pass laws requiring any corporations doing business in this state to comply, within five days of service, with compulsory process from proper authorities in this or other states

seeking information and records of electronic communication services or remote computing services located outside New Jersey. Alternatively, New Jersey should encourage a new interstate compact that would help ensure enforcement of out-of-state subpoenas and warrants stemming from Internet investigations.

ONLINE PRIVACY

- By formal resolution, and in cooperation with the State's Executive Branch, the New Jersey Legislature should call upon the federal government to enact and implement the following new federal laws, enforced by the Federal Trade Commission (FTC), to enhance privacy in cyberspace:

  - Web sites, online vendors and interactive computer services should be prohibited from collecting or storing information regarding subscribers or customers without proper protection of privacy interests. Unless dissemination of the information collected is necessary to further the customer/vendor commercial relationship, the subscriber or customer should be fully informed of the potential dissemination and given an opportunity to preclude it ("opt out") by withholding consent. A procedure should be established to inform the subscriber or customer of the information maintained about him or her and to permit correction of any errors. The law should require the FTC to promulgate regulations to protect the privacy of the personal information collected over the Internet from or about private individuals who are not covered by the Children's Online Privacy Protection Act of 1998. State attorneys general should be authorized to bring federal actions against violators upon giving notice to the FTC.

  - Using, or causing to be used, an electronic mail service provider's system in violation of its policy prohibiting or restricting the use of its service or equipment for unsolicited electronic mail commercial advertisements should be prohibited. Providers should be afforded significant civil remedies against violators, including liquidated damages set forth in the statute and attorney's fees.

  - Sending unsolicited commercial electronic mail to another person should be prohibited if the other person asks that it not be sent. Specifically, the law should forbid failing to comply with the request of a recipient of unsolicited e-mail, delivered to the sender's e-mail address, to stop sending such messages. The law also should require the person initiating any such e-mail to provide a bona fide name, physical address, e-mail address and telephone number, as well as notice that no further transmissions will occur upon receipt of a request to end them. Civil remedies

should be afforded to state attorneys general and aggrieved private individuals.

- ♦ Sending unsolicited e-mail containing a false or misappropriated name of the sender, e-mail return address, or name and phone number of a contact person should be prohibited. The law also should bar sending an unsolicited e-mail to an interactive computer service with knowledge that the message falsifies an Internet domain, header information, date or time stamp, originating e-mail address or other identifier. Lastly, the law should forbid using, creating, selling or distributing any computer software that creates on an e-mail message false Internet domain, header information, date or time stamp, originating e-mail address or other identifier.

- New Jersey should enact a law prohibiting public, charter and private schools from disclosing personal information about students on their Web sites without first receiving parental consent to the extent allowed under the federal Family Educational Rights and Privacy Act.

RESTRAINING ONLINE SALES

- Consideration should be given to adopting legislation to authorize the New Jersey State Board of Pharmacy in the Division of Consumer Affairs to license out-of-state pharmacies doing business with New Jersey residents over the Internet.

- A new federal law should be passed permitting state attorneys general to seek injunctive relief in federal court against those violating state laws regulating Internet sales of intoxicating liquor and tobacco.

- Federal legislation should be adopted prohibiting the sale of guns, ammunition or explosives over the Internet.

ESTABLISH AND PUBLICIZE HOTLINES AND COMPLAINT PROCESSES

- The Statewide Computer Crime Task Force should set up a 24-hour toll-free hotline telephone service to receive complaints of computer-related crime. The number should be publicized as a place to report online child pornography, cyber-stalking, threats of violence in schools or elsewhere, online fraud, and unauthorized intrusions into computer systems.

- The Department of Law and Public Safety’s Web site for safe

computing guidelines should include electronic forms for filing complaints of computer-related wrongdoing with enforcement agencies.

MAINTAIN PROHIBITION ON INTERNET GAMBLING

- As an unauthorized form of gambling, Internet gambling is illegal in New Jersey, and the prohibition on such gambling should be maintained.

- New Jersey should not encourage additional legalized gambling and should continue to support passage of Senator Kyl's Internet Gambling Prohibition Act of 1999 ("Kyl Bill") and its House equivalent by Congress. New Jersey should similarly support stringent enforcement of the Kyl Bill as well as the 1961 Federal Wire Act as it pertains to Internet gambling.

- As one of the means of enforcing a prohibition of Internet gambling by New Jerseyans, specific legislation addressing the issue should be considered. For example, it may be possible to develop legislation that would discourage credit card and other financial service companies from providing the means to engage in illegal Internet gambling.

- In the event a federal prohibition of Internet gambling is not enacted, and state attempts at prohibition prove to be ineffective or contrary to New Jersey's interests, the regulation of Internet gambling should expeditiously be reconsidered.

*** * ***

The State Commission of Investigation and the Attorney General wish to extend special thanks to the following staff who assisted in the preparation of the joint public hearing and this report:

- **Robert J. Clark, Deputy Director, State Commission of Investigation**

- **Christopher G. Bubb, Chief, Computer Analysis and Technology Unit, Division of Criminal Justice**

- **Brian J. Litten, Chief Legislative Counsel, Office of the Attorney General**

- **Amy E. Melick, Legislative Counsel, Office of the Attorney General**