

# Internet Fraud Cybercrime II

## In This Issue

May 2001  
Volume 49  
Number 3

United States  
Department of Justice  
Executive Office for  
United States Attorneys  
Office of Legal Education  
Washington, DC  
20530

Mark T. Calloway  
Director

Contributors' opinions and  
statements should not be  
considered an endorsement  
by EOUSA for any policy,  
program, or service

The United States Attorneys'  
Bulletin is published pursuant  
to 28 CFR § 0.22(b)

The United States Attorneys'  
Bulletin is published bi-  
monthly by the Executive  
Office for United States  
Attorneys, Office of Legal  
Education, 1620 Pendleton  
Street, Columbia, South  
Carolina 29201. Periodical  
postage paid at Washington,  
D.C. Postmaster: Send  
address changes to Editor,  
United States Attorneys'  
Bulletin, Office of Legal  
Education, 1620 Pendleton  
Street, Columbia, South  
Carolina 29201

**Managing Editor**  
Jim Donovan

**Assistant Editor**  
Nancy Bowman

**Law Clerk**  
Todd Hagins

**Internet Address**  
[www.usdoj.gov/usao/  
eousa/foia/foiamanuals.html](http://www.usdoj.gov/usao/eousa/foia/foiamanuals.html)

Send article submissions to  
Managing Editor, United  
States Attorneys' Bulletin,  
National Advocacy Center  
Office of Legal Education  
1620 Pendleton Street  
Columbia, SC 29201

- Interview with Michael W. Bailie, Director, Office of Legal Education** . . . . . 1
- The Rising Tide of Internet Fraud** . . . . . 6  
By Jonathan Rusch
- Tracking a Computer Hacker** . . . . . 13  
By Daniel A. Morris
- Tracing in Internet Fraud Cases: PairGain and NEI Worldwide**  
By Christopher M.E. Painter
- Communications Assistance for Law Enforcement Act (CALEA)**  
By CALEA Implementation Section
- Novel Criminal Copyright Infringement Issues Related to the Internet** . . . . . 33  
By David Goldstone and Michael O'Leary
- The Economic Espionage Act of 1996: An Overview** . . . . . 41  
By George "Toby" Dilworth
- It's Not Just Fun and "War Games" — Juveniles and Computer Crime** . . . 48  
By Joseph V. DeMarco
- The Computer and Telecommunications Coordinator (CTC) Program** . . . 55  
By Stacey Levine

---

---

# Interview with Michael W. Bailie



Michael W. Bailie began his legal career with the Department of Justice in 1979 as an Attorney-Advisor in the Justice Management Division. He joined the

Executive Office for United States Attorneys (EOUSA) in 1988 as an Assistant Director for Office Automation. Since that time, he has held a number of positions with the EOUSA, culminating in his appointment as Director of the Office of Legal Education (OLE) in 1997. He supervised the move of the OLE from Washington, D.C. to the National Advocacy Center in Columbia, South Carolina in April 1998.

Mr. Bailie (MB) was interviewed by Jim Donovan (JD), Managing Editor of the United States Attorneys' Bulletin.

**JD:** How did you develop an interest in 1979 in technology and what experience did you have at that time?

**MB:** I didn't have any experience. I was just coming out of law school and I was looking for a job. Actually, at that point in time, it seemed interesting and I stayed involved with the technology for about ten years.

When I came to the Executive Office for United States Attorneys (EOUSA), the districts had twelve different word processing systems. We couldn't exchange information between United States Attorney's Offices (USAO) so it was a real mess. My job was to replace the word processing systems with PCs that were compatible. Shortly after I came onboard, they awarded the Eagle Contract and installed the first nationwide

computer system for USAOs. We have come a long way since then.

**JD:** Nobody had desktop computers at that time?

**MB:** No. When I came to EOUSA in 1988 there were only 600 PCs throughout the country in USAOs for a workforce of about 8,000 or 9,000 people. Most of the attorneys did not have any type of word processing capabilities on their desks.

**JD:** Did you foresee at that time the technological wave of the future?

**MB:** I didn't realize the extent to which PCs would be installed in the USAOs or the role that e-mail would play. Today, you go without e-mail for a couple of hours and it's like you are having withdrawal.

**JD:** How do you feel your background has prepared you for your current position as Director of the Office of Legal Education?

**MB:** When I was Deputy Director of Operations in EOUSA, I was responsible for many different aspects of administration in USAOs and that included facilities, technology, communications, budget, personnel, and office automation. I used to refer to it as Deputy Director of Mops and Brooms. When I came to the NAC, I was ready to deal with all the different aspects of running a large building complex and conference center. What I wasn't prepared for was being a hotel manager. For the most part though, the background that I had in the EOUSA and in the Department prepared me for many of the administrative aspects associated with putting together a viable training program, as well as efficiently running the conference center.

**JD:** You recently received a very prestigious award. Why don't you describe that for us.

**MB:** The award really should have gone to the staff. It was a Presidential Rank Award that is given to members of the SES around the country. I was certainly honored to receive it, but the reason I received it was because of the work that

---

OLE has done here in Columbia. We have fifty people here that do a tremendous job on a day-to-day basis and are dedicated to making this the best training facility in the United States. I think that they are succeeding.

**JD:** You have been at the National Advocacy Center (NAC) since its inception. What is the mission of the NAC?

**MB:** Our charter is to provide legal education and training to the federal legal community. That involves providing training and educational services to the Department of Justice and USAOs, as well as the lawyers that are in the Executive Branch of the government. We train about 15,000 people per year at the NAC.

**JD:** Has the mission of the NAC changed over the three years that it has been in existence?

**MB:** No. Our job here is to provide the substantive knowledge that our attendees need to do their jobs on a daily basis. At the same time it is our belief that if we make people as comfortable as possible, they will not focus on satisfying their creature comforts, but will focus on learning.

**JD:** Were you apprehensive, at all, about asking the Assistant United States Attorneys (AUSAs) from around the country to come to training in one central location when they previously had been able to train in different cities throughout the United States?

**MB:** Yes, I think we were all apprehensive. There was a lot of talk from AUSAs before we opened that they did not want to come to South Carolina. They saw it as perk of their job that they could go to other locations. Our primary focus in the beginning was to show them that this was going to be a great place to learn. Our philosophy was to bring in the people that could carry the message back to their offices that this was a premier facility. When we did the first course here, we invited First Assistant United States Attorneys (FAUSAs) and did a one and one-half day program to show them that it was not going to be bunk beds and dorm rooms and that we had a state-of-the-art training and educational facility. The FAUSAs went back to their offices and spread the word. Some people were still skeptical and we continued to enhance the facility. We are

still making improvements on a daily basis. Our students have been happy with what we have done here. We hear very few complaints from anybody these days. We might get one evaluation out of 250 that asks why the seminars aren't held in New Orleans or Washington, but those are few and far between.

**JD:** Has the move to the NAC changed the operations of OLE?

**MB:** Yes, in a positive way. In the old days we used to have our materials printed, then we would pack them up and ship them out to the location. We would send our staff to a hotel where we would attempt to convert a hotel ballroom into a classroom. We would have to rent AV equipment, easels, etc. It was a logistical nightmare. Now, everything is here. We even have our own printing facility. It is run by South Carolina Vocational Rehabilitation Program. We print about 1.8 million copies per month. The seminar binders are put together here and they are wheeled to the courtrooms. All of our AV equipment is in place and is state of the art. All of our taping facilities are here. We have the classrooms in place and we can assure that the lighting and sound is proper. We also have video teleconferencing (VTC) equipment here that we would not have had in a hotel. We can do hands-on computer training at the NAC. Centralized training offers us a multitude of advantages over the way that we used to do things.

**JD:** With the move to South Carolina, have you had any trouble in bringing in quality instructors or judges for your volunteer faculty?

**MB:** No, we haven't had any problem. In fact, we probably have more people than we can use. We have many people who are continuously volunteering. We even have District Court Judges booked in the Center through October of this year.

**JD:** One initial complaint about having the NAC in Columbia was the difficulty in getting direct flights in and out of Columbia, South Carolina. I know that you have put a great deal of time and effort into making travel connections a lot easier to arrange. How is that going?

**MB:** We have worked very well with the local community and with the Columbia Metropolitan

---

Airport and the Airport Authority to provide them information regarding the number of people attending our seminars. They have used that information to show the airlines that we can put bodies in seats on flights to Columbia. The 15,000 people per year who attend classes at the NAC are large numbers when you talk to an airline, especially a regional carrier. We have been successful in helping to bring another thirty or so additional flights into Columbia per day and now we have fifteen or sixteen cities that have direct air service into Columbia. Before the NAC opened there were no direct flights from Washington, D.C. to Columbia and now we have seven a day.

**JD:** Have you had any pleasant surprises as a result of the training taking place in one central location at the NAC?

**MB:** I think the most beneficial thing that I have seen happen here is that people are forced to communicate with one another. When we had training in Washington, people would eat breakfast and lunch separately and go their own way at night or hook up with friends in the city when they were attending a course. Here, they are forced to eat with and talk to one another. With four or five or six courses going on at any given time, there is a large variety of people in the Center and a great camaraderie has developed as a result of forcing people to learn in a single facility. When we see people hugging one another as they are leaving after making friends during the course of a week, that is when we know that we have done the right thing. One particular example I can think of occurred at a criminal trial advocacy course that was run by DOJ at the same time that a Beginning Trial Advocacy Course was held by the National District Attorneys' Association (NDAA). People in both of these classes were relatively new attorneys and they bonded. As they were leaving on Friday at noon, they were standing around hugging one another and exchanging business cards. I thought at the time that this is what it is really all about. The exchange of information, the exchange of ideas, and working together is the reason that we are really here in one central location. That is probably the most beneficial aspect of our location.

**JD:** Has the NAC encouraged joint training of state and local prosecutors and state and federal law enforcement?

**MB:** Yes, we have had a number of courses that we have developed jointly with the NDAA and National Association of Attorneys General. These courses have been in the areas of internet fraud, telemarketing fraud, international issues, and ethics. They have helped us with our forensics course and provided instructors. All of our courses are open to state, local, and federal attorneys. It is just a question of how much room we have in each course. We have also encouraged international training and have conducted several courses for foreign prosecutors, primarily from South America. We have also provided courses for Canadian and Mexican prosecutors.

**JD:** At the present time, do you have the ability to pull up the course catalog on the internet/intranet site?

**MB:** Right now users have the capability of bringing up an agenda on our website. It is pretty general in nature, but it will show attendees the topics that were covered in the last course.

**JD:** You have added more hands-on computer courses in the past couple of years. What needs do you think hands-on courses meet that possibly haven't been met previously?

**MB:** Originally when we moved here we had one small computer training room. We have since expanded that training room and added a second computer training room to do systems training. We also modified our largest classroom to accommodate lap tops so we can have 90 lap tops in that room at any given time. There are a number of courses that we are offering, such as cybercrimes, internet fraud, and child exploitation where it is beneficial to have AUSAs and, in some cases, investigators, sit together and actually access the internet to see how the criminals are using the technology. We will probably take a look at either modifying more of our classrooms or at wireless solutions in order to hand PCs to people to use while they are participating in that particular course.

**JD:** How do you determine what courses you are going to offer at the NAC or whether it is time to

---

---

change or revise a course that has been offered over a period of time?

**MB:** Each year we survey all the USAOs, all the legal divisions, and our client agencies and ask them to provide us input into our course calendar. We have already received a lot of great ideas for our FY 2002 calendar. Once we have amassed all of the suggestions, we meet with our Assistant Directors (ADs) to review and discuss the suggestions. We do have limitations on the number of people that we can bring into the building and the size of the courses. Over the last three years, OLE has offered approximately 175 courses per year at the NAC.

**JD:** Do you have a lot of freedom to make changes at the NAC?

**MB:** We could not have done any of this without the support of EOUSA and the Directors that have been involved in this process. They have allowed us to think outside the box, to try new and different things, and much of the success of the NAC has been the result of things they have allowed us to do here. The credit goes to Washington for having enough vision to allow us to do what was necessary to get the job done.

**JD:** Would it be fair to characterize the NAC as a work in progress in that there seems to be a continual effort to get the word out to federal employees?

**MB:** Yes, the NAC is a work in progress. There are things that we find every day that we can do to both improve the quality of training that we offer here, as well as the quality of life that we provide. If we can do something in a classroom to enhance an instructor's performance, we will do that, whether it is offering a portable PC with presentation software already available, upgrading the equipment that we have in the courtrooms, or giving them a fluffier pillow in their hotel room.

**JD:** What do you see in the future for the NAC?

**MB:** We intend to tailor our live courses for our clientele recognizing that they are becoming more and more experienced. We find that most of the AUSAs that attend our courses have more than ten years of experience. Rather than concentrating on basic principles, we are looking to focus our

courses on areas of the law that are of greater importance to those people with extensive experience. We are planning a series of symposiums for our experienced AUSAs that would involve bringing in twenty or twenty-five prosecutors to talk about a specific topic, such as capital litigation. We are also going to be focusing more attention on the use of technology. We offer a course here that is called Information Technology and Litigation Investigations and we can't offer it enough. We also offer several courses in litigation support for paralegals and support staff. People are clamoring to get into those courses. The use of technology in the courtroom and in the investigative process is expanding tremendously. As a result, I think we have to meet those needs.

**JD:** The NAC has a number of different aspects to its educational program including, most obviously, the seminars and the instructors that are brought in, but it seems that there is an increasing emphasis recently on the Distance Education Program. Could you describe that for us?

**MB:** We have found that we can only train so many people here in South Carolina as a result of our physical limitations, that is, the number of classrooms and hotel rooms here at the NAC and in Columbia. Consequently, we have come up with a five-prong approach to distance education that we are in the process of implementing today. Our distance education plan includes video and audio tape training, web-based training to include a virtual university, a satellite network, Video Tele-Conferencing (VTC), and interactive CD-ROM. The satellite network will be available to every employee of the USAOs on a variety of subjects. We are in the process of installing satellite dishes in all 220 of our staffed branch offices for USAOs. We are also looking at doing some CD-Rom-based training which is another way of reaching our audience, as well as the use of VTC in a brown-bag lunch format. The VTC has interactive capabilities and that is already installed throughout the United States. We also anticipate using a combination of these methods such as having an instructor provide a lecture on VTC to our studio here in Columbia and then broadcasting that lecture over the satellite

---

network. It will be mix and match as we go. The distance education program is not meant to replace our live training, which we believe will always be our bread and butter, but it will serve as a supplement to our live training here at the NAC.

**JD:** You indicated that there are approximately 220 satellite hook-ups now?

**MB:** There will be 220. As of today, we have 66 that are operational.

**JD:** What is the time frame for having them all up?

**MB:** Yesterday. We would have liked to have had them all installed by this time. That was our intent. We have run into a few problems installing dishes on roofs of government and non-government buildings. Hopefully, within the next month, we will have them all available.

**JD:** Will that then connect every USAO and every USAO branch office to the NAC?

**MB:** Every staffed branch office will have access to the Justice Television Network (JTN).

**JD:** What sort of programs are you going to broadcast over this system?

**MB:** Our plan is to provide a variety of programs. We will broadcast programs that cover substantive areas of the law. We will also provide information to USAOs, concerning news, updates on cases, recent decisions by the courts, administrative information and training on topics such as sexual harassment and AIDS awareness, and computer security. We hope to also be able to offer panel discussions on a variety of topics. We have installed an 800 number in the Advocacy Center Studio so people will be able to call in and ask questions. That is important in terms of being able to get continuing legal education credits from the state bars. Most state bars are now telling us that we need to have a moderator and we need to be able to answer questions for the attendees at those courses to receive CLE credits.

**JD:** Could you expand on the use of VTC for training?

**MB:** The theory behind VTC, originally, was that we would be able to do a one hour, brown-bag lunch on a particular topic and broadcast it to

fourteen or fifteen sites at one time. We tried that a couple of times and it turns out that a better use of VTC, because of the technology involved, is to combine it with the use of our satellite. That involves having instructors appear by way of VTC and then using the satellite to broadcast the lecture. The satellite is much more sophisticated in terms of quality of audio and video. We do use VTC for our live courses when we can't get an instructor here for one reason or another. The VTC allows us to have that instructor appear in the classroom with the students and answer questions. The interactive capabilities of that technology are the most important aspect of VTC.

**JD:** You also mentioned the concept of virtual university. Why don't you expand on that?

**MB:** The virtual university concept is being used by a number of federal agencies and basically it allows every user with a password to access courses on the Internet. The theory is that we would give every employee in USAOs a card with an ID number, and that would allow that person to select one of over 400 courses that are available, and take that course online. It would be interactive and include audio and video. You would be able to proceed at your own pace through that course. It would be available twenty-four hours per day, seven days per week. If you wanted to take a course on leadership, you could log on and if you could only spend an hour taking that course before work started, then you could sign off and pick it up again five hours or two days later. The administrator of the course would be able to track your progress. As you completed each course, it would be noted under your ID and then the administrator could print off all the courses you have taken during the year. It is relatively inexpensive. It would be customized for DOJ and USAO employees. We are also working with the University of South Carolina (USC) to provide college credits for support staff courses that we offer here at the NAC. The USC is presently looking at our agendas and course materials for topics like advanced paralegal, experienced legal secretaries, support staff supervisors, and other subjects to see if we can't get accreditation for those courses.

---

**JD:** How close to reality is the virtual university program?

**MB:** We have already tested that concept. We had about one month of testing here and the Systems Managers in the USAOs are also testing it. I think that it is probably within three to six months of becoming a reality.

**JD:** Why the five-prong approach? Why not focus all of your attention on the satellite or one of the areas that you mentioned?

**MB:** We looked at the various capabilities of distance learning and we also considered the way people learn. Everyone learns differently. Some people learn better by sitting in their car driving from Butte to Billings and listening to an audio tape. Some learn better sitting in a two-hour session watching a television program. Some prefer sitting in front of a computer and going through an interactive web program at their leisure. We thought that by offering all of these alternatives, in various forms, that we would be able to meet the diverse needs of all of our users.

---

## The Rising Tide of Internet Fraud

*Jonathan Rusch*

*Special Counsel for Fraud Prevention  
Fraud Section of the Criminal Division*

By all accounts, the United States leads the world in using the Internet for commerce and communication, and in spending on electronic commerce. There are growing indications that along with the expansion of legitimate Internet use, the United States is experiencing a rising tide of fraud that exploits the Internet.

The Internet Fraud Complaint Center (IFCC) – a joint project of the FBI and the National White Collar Crime Center – reported that in its first six months of operation, May-November 2000, it had recorded more than 37.5 million hits on its Website and had received more than 20,000 complaints from the public. Of those complaints 5,273 were Internet fraud-related complaints that it referred to law enforcement for possible investigation. *See* Internet Fraud Complaint Center, Six Month Trends Report: May - November 3 (2000) *available at* <http://www.ifccfbi.gov/strategy/6monthreport.pdf>. Moreover, more than 90 percent of all complainants whose complaints were referred for possible investigation, and more than 90 percent of all alleged perpetrators named in complaints referred for possible investigation, were located in the United States. It should be noted that because

the IFCC has been in operation for less than a year, these statistics may be affected by several variables (e.g., the extent of public recognition of Internet fraud as a crime, the manner in which the public is being solicited to file complaints, and the extent to which the public identifies IFCC as an appropriate contact for complaints) and may not be fully representative of the number and frequency of various types of Internet fraud. More recently, the 2001 Computer Crime and Security Survey, a joint project of the Computer Security Institute and the FBI, reported that in 2000, financial fraud was the second-leading category of financial losses due to computer use – second only to theft of proprietary information – and accounted for nearly \$93 million in losses. *See* Press Release, Computer Security Institute, Financial Losses Due to Internet Intrusions, Trade Secret Theft, and Other Cyber Crimes Soar (May 12, 2001) *available at* [http://www.gocsi.com.prelea\\_000321.htm](http://www.gocsi.com.prelea_000321.htm).

Other countries are also seeing a substantial increase in various categories of Internet fraud. In December 2000, the International Chamber of Commerce's Commercial Crime Services (CCS) Division reported that Internet fraud in 2000 was "rising dramatically," accounting for more than two-thirds (2,776) of the 4,139 cases that its business partners referred – more than twice as many as in 1999. *See* Press Release, International

---

Chamber of Commerce, Dramatic Rise in Web-Based Fraud Reported (Dec. 2000) *available at* [http://www.iccwbo.org.ccs/news\\_archives/2000/du\\_e\\_diligence\\_for\\_web.asp](http://www.iccwbo.org.ccs/news_archives/2000/du_e_diligence_for_web.asp). In a February 2001 report, the European Commission (EC) stated that credit card fraud in the European Union had risen by 50 percent in 2000 to \$553 million in illegal transactions, and that the increase was greatest for "card-not-present" transactions (i.e., mail-order, telephone, and Internet sales), especially on the Internet.

These substantial worldwide increases may be attributable to significant increases in worldwide Internet access. Between March and October 2000, Internet access in European Union households grew 55 percent (from 18 to 28 percent of all households), according to EC data released March 13, 2001. The EC also noted that Europe now has about as many Internet users as the United States.

The emerging data suggests that the problem of Internet fraud is becoming uniquely global in scope and impact, as criminals can plan and execute fraudulent schemes from anywhere in the world and victims may be located anywhere in the world. It is noteworthy that in the IFCC's first six months of operation last year, it received complaints from persons in 106 different countries.

### **Fraud Involving Online Auctions**

Data from the IFCC, the Federal Trade Commission, and Internet Fraud Watch (a project of the non-profit National Consumers League) show that fraud involving the use of online auctions is by far the most frequently reported type of Internet fraud. The IFCC, for example, reports that more than 64 percent of all referred complaints involved online auctions.

Online auction fraud typically involves several recurring approaches. The most common approach appears to be the offering of some valuable item, such as computers, high-priced watches, or collectible items, through a known online auction site. The individuals who are informed that they are successful bidders send their money to the seller, but never receive the promised merchandise. In a variation of this

approach, the criminals send counterfeit merchandise in place of the promised merchandise. A third approach involves the criminal contacting losing bidders in a particular online auction, informing them that additional units of the item on which they bid have become available, and taking the bidders' money without delivering the items.

Two additional aspects that are unique to online auctions are "shill bidding" and "shill feedback." "Shills" are bidders who have no genuine interest in the merchandise on which they are bidding, but have been hired to place bids in order to create an appearance of interest and prompt genuine bidders to bid higher than they might have otherwise. In online auctions, criminals can take advantage of multiple e-mail addresses and false identities to place shill bids.

Consumers interested in a particular auction sometimes want to learn if other buyers have had favorable experiences with the purported seller in that auction. Major auction sites like eBay and Amazon.com allow legitimate customers to provide feedback on their experiences with particular sellers. Criminals, however, can also use false e-mail identities to provide "shill feedback" – false favorable information about themselves – to make it appear that they are satisfied customers and to give consumers a false sense of security about that auction.

In a recent prosecution, *United States v. Denlinger*, No. 00CR573IEG (S.D. Cal. filed Feb. 28, 2000), the defendant used online auction sites to offer Beanie Babies for sale, but failed to deliver the products after receiving the victim's money. He used various "screen names" (or aliases) in sending e-mails to prospective victims, and provided them with screen names and e-mail addresses of persons he falsely described as "references." In fact, those screen names were assigned to the defendant, so that when victims e-mailed the "references," the defendant responded with messages that gave victims false and favorable information about his own reliability and trustworthiness as a seller. The defendant also used two techniques to prevent victims from contacting him directly: he gave victims a pager number and falsely told them it was his home

---

telephone number; and he asked them to send their payments to various commercial mail receiving agencies, which he falsely told them was his home address. His scheme defrauded more than 200 victims of nearly \$50,000. (The defendant, after pleading guilty to mail and wire fraud, was sentenced to twelve months imprisonment and \$46,701 in restitution.)

### **Fraud Involving Online Retail Sales**

One category of fraud that overlaps with auction fraud is fraud in online retail sales of goods and services. The IFCC reports that so-called "nondeliverable" merchandise accounts for 22 percent of all referred complaints. One approach to retail fraud has involved placing banner advertisements on an auction site that offers the same types of goods being auctioned. Prospective buyers who click on the banner advertisement are taken to a different Website that is not part of the auction site, and that offers none of the protections that leading auction Websites have adopted for their members. Another approach involves using unsolicited commercial e-mail ("spam") to lure prospective victims to a Website which purports to sell items of the same type that are available through well-known online auction sites.

In retail sales of services, some criminals have taken advantage of the complexities of the Internet's operations to compel or mislead consumers into visiting their Websites. In *United States v. Kashpureff*, 98CR0218 (E.D.N.Y. filed March 19, 1998), the defendant operated a Website, AlterNIC, that competed with the InterNIC Website for domain name registration. He wrote and placed software on that Internet that caused persons who wanted to visit the InterNIC Website to be involuntarily redirected to his Website. Ultimately, he pleaded guilty to a violation of the computer fraud statute, 18 U.S.C. § 1030.

In *United States v. Lee*, No. 99-00560 SOM (D. Haw. filed Dec. 9, 1999), the defendant knew that the Hawaii Marathon Association operated a Website with the Uniform Resource Locator (URL) "www.hawaiimarathon.org" to provide information about the Marathon and enable runners to register online. Although he had no

affiliation with the real Hawaii Marathon, he copied the authorized Marathon Website, and created his own Website with the confusingly similar name, "www.hawaiimarathon.com." Runners who came to his Website thinking that it was the real Hawaii Marathon site were charged a \$165 registration fee – \$100 more than the real site charged for entry. The defendant also operated another Website where he sold Viagra over the Internet without a prescription. (The defendant later pleaded guilty to wire fraud and unlawful sale of Viagra, and in February 2001 was given a split sentence of ten months imprisonment.)

### **Investment Fraud**

Another major category of online fraud is investment fraud. The Securities and Exchange Commission (SEC) has reported that it receives between 200 and 300 online complaints each day about possible securities fraud online. While the major types of online securities fraud generally parallel traditional securities fraud schemes, market manipulation schemes are a frequent focus of enforcement actions.

"Pump-and-Dump." The most widely publicized form of online market manipulation is the so-called "pump and dump" scheme. In a "pump and dump," criminals identify one or more companies whose stock is thinly traded or not traded at all, then adopt various means to persuade individual online investors to buy that company's stock. These means can include posting favorable, but false and misleading, representations on financial message boards or Websites, and making undisclosed payments to people who are ostensibly independent but who will recommend that stock. Once the price has increased sufficiently, the participants in the scheme – who may be company insiders, outsiders, or both, sell their stock, and the stock price eventually declines sharply, leaving uninformed investors with substantial financial losses. While an outsider who merely expresses his opinions about the worth or likely increase or decrease of a particular stock may not be committing criminal fraud, outsiders or insiders whose conduct extends beyond mere advocacy to manipulation of markets for their personal profit by giving the public false and

---

misleading information may violate securities fraud statutes and other criminal statutes.

In one pump-and-dump case, *United States v. Aziz-Golshani*, No. 00-007-GAF (C.D. Cal. filed Jan. 4, 2000), two defendants manipulated the stock of a bankrupt company, NEI Webworld, Inc. They posted messages on several financial message boards, falsely stating that NEI was going to be taken over by a California company, and, with the help of a third individual, bought 130,000 shares of NEI before their manipulations resulted in a dramatic price increase. In an attempt to conceal their identities, the two defendants and their confederates used computers at the UCLA Biomedical Library to post the false reports. An SEC amended complaint charged that the defendants and another individual had also engaged in similar manipulative conduct concerning the securities of eleven other issuers in 1999. (In January, 2001, both defendants were sentenced to fifteen months and ten months imprisonment, respectively).

"Cybersmear." The converse of the "pump and dump" is the "cybersmear." A "cybersmear" scheme is organized in the same basic manner as a "pump-and-dump," with one important difference: the object is to induce a decline in the stock's price, to permit the criminals to realize profits by short-selling. To accomplish a sufficiently rapid decline in the stock's price, the criminal must resort to blatant lies and misrepresentations likely to trigger a substantial sell off by other investors.

In *United States v. Moldofsky*, No. S100CR388 (RPP) (S.D.N.Y. convicted March 8, 2001), the defendant, a day trader, on the evening of March 22, 2000, and the morning of the next day, posted a message nearly twenty times what was designed to look like a Lucent press release announcing that Lucent would not meet its quarterly earnings projections. For most of those postings, he used an alias designed to resemble a screen name used by a frequent commentator on the Lucent message board who had historically expressed positive views of Lucent stock. He also posted additional messages, using other screen names that commented on the release or on the message poster's conduct. On March 23, Lucent's stock price dropped more than 3.7

percent before Lucent issued a statement disavowing the false press release (*See* [www.sec.gov/litigation/litreleases/lr6493.htm](http://www.sec.gov/litigation/litreleases/lr6493.htm)), but rose by 8 percent within ten minutes of Lucent's disavowal.

In *United States v. Jakob*, No. CR-00-1002-DT (C.D. Cal. indictment filed Sept. 28, 2000; pleaded guilty Dec. 29, 2000), the defendant engaged in even more elaborate fraudulent conduct to effect a "cybersmear." After he tried to short-sell stock in Emulex, but found that the market was bidding up the price, he wrote a press release falsely reporting that Emulex was under investigation by the SEC, that Emulex's Chief Executive Officer was resigning, and that Emulex was reporting a loss in its latest earnings report. He then caused his former employer, a company that distributed online press releases, to send it to major news organizations, which reported the false statements as fact. When Emulex stock rapidly declined, the defendant covered his short-sale position by buying Emulex stock and realizing nearly \$55,000 in profits. He also bought more Emulex stock at lower prices, and sold when the stock had recovered most of its value.

One notable feature of online market manipulation schemes is the speed with which the scheme's participants can induce dramatic, though short-term, fluctuations in stock prices, and can realize substantial profits by correctly timing their purchases and sales. In *Aziz-Golshani*, during the week of November 9, 1999, the defendants bought their NEI stock at prices ranging from 9 cents to 13 cents per share. On November 15, 1999, NEI stock opened at 9:00 a.m. Eastern time at \$8 per share, and within 45 minutes had risen to \$15 5/16 per share. Less than a half-hour later, NEI stock had dropped to approximately 25 cents per share. By selling when the stock price was still high, the defendants realized profits of more than \$360,000. In *Jakob*, once the false press release was distributed, Emulex's stock price dropped in less than one hour from more than \$110 per share to approximately \$43 per share, and the trading volume of Emulex stock increased significantly as individual traders sold off the stock at notably lower prices. The defendant realized nearly \$55,000 in profits from his short sale, and

---

additional profits of nearly \$187,000 as the stock price rebounded.

### **Payment Card Fraud**

One of the fastest-growing categories of Internet fraud is payment card (i.e., credit card and debit card) fraud. One Internet research firm, Meridien Research, predicted in January 2001 that online payment-card fraud worldwide will increase from \$1.6 billion in 2000 to \$15.5 billion by 2005.

Online credit card fraud causes substantial problems for online merchants. Initially, many online merchants were defrauded when people, using others' credit card numbers, ordered merchandise and had it shipped to foreign locations that were clearly different from the addresses of the true credit card holders. Under the policies that major credit card issuers established, merchants must bear the losses for online purchases, which qualify as "card-not-present" transactions. As a number of merchants took defensive measures, such as installing software designed to flag possibly fraudulent online transactions, some criminals changed their methods to request shipment of the goods they ordered with others' credit card numbers to United States addresses. Confederates then sell or ship those goods to another location.

To commit online payment-card fraud, criminals need access to valid payment-card numbers. One means of acquiring them is the unlawful accessing of e-commerce Websites. Within the past year, several computer intrusions that made possible the downloading of tens of thousands, if not millions, of credit card numbers – such as the exposure of more than 3 million credit cards at Egghead.com – have received worldwide attention in the media.

A number of Internet credit card schemes involve computer hacking as the means of accessing the numbers. For example, in *United States v. Bosanac*, No. 99CR3387IEG (S.D. Cal. filed Dec. 7, 1999), the defendant was involved in a computer hacking scheme that used home computers for electronic access to several of the largest United States telephone systems and for downloading thousands of calling card

numbers (access codes). The defendant, who pleaded guilty to possession of unauthorized access devices and computer fraud, used his personal computer to access a telephone system computer and to download and transfer thousands of access codes relating to company calling card numbers. In taking these codes, the defendant used a computer program he had created to automate the downloading, and instructed his coconspirators on how to use the program. The defendant admitted that the loss suffered by the company as a result of his criminal conduct was \$955,965. He was sentenced to eighteen months' imprisonment and \$10,000 in restitution.

Computer intrusions, however, are by no means the only way for criminals to obtain payment-card numbers for online fraud. In addition to traditional methods such as "dumpster diving" (i.e., sorting through trash to find credit card bills or receipts), they can go to Websites where others have posted credit card numbers, and even use credit card generator programs such as Credit Master, Credit Wizard, and Credit Probe. These programs can generate batches of potentially valid credit card numbers based on the algorithm that credit card issuers use to validate their account numbers. In some instances, criminals have engaged in identity theft by using publicly available identifying data of others to obtain credit card numbers in the victims' names (see below).

### **Identity Theft and Fraud**

Online payment-card fraud is closely related to the problem of identity theft and fraud. The Federal Trade Commission (FTC) reports that its Consumer Sentinel Website, which provides law enforcement with access to more than 300,000 complaints about all types of consumer fraud, has received more complaints about identity theft and fraud than any other category of consumer fraud. (See [www.consumer.gov/sentinel/trends.htm](http://www.consumer.gov/sentinel/trends.htm).) While identity theft can be committed in furtherance of many types of crime, a number of recent federal prosecutions have combined identity theft and Internet fraud.

In *United States v. Christian*, No. 00-03-SLR (D. Del. filed Aug. 3, 2000), two defendants obtained the names and Social Security numbers

---

of 325 high-ranking United States military officers from a public Website, then used those names and identities to apply for instant credit at a leading computer company and to obtain credit cards through two banks. They fenced the items they bought under the victims' names, and accepted orders from others for additional merchandise. The two defendants, after pleading guilty to conspiracy to commit bank fraud were sentenced to thirty-three and forty-one months imprisonment and restitution of more than \$100,000 each.

Similarly, in *United States v. Wahl*, No. CR00-285P (W.D. Wash. sentenced Oct. 16, 2000), the defendant obtained the date of birth and Social Security number of the victim (who shared the defendant's first and last name and middle initial). He then used the victim's identifying information to apply online for credit cards with three companies and to apply online for a \$15,000 automobile loan. He actually used the proceeds of the automobile loan to invest in his own business. (The defendant, after pleading guilty to identity theft, was sentenced to seven months' imprisonment and nearly \$27,000 in restitution).

### **Business Opportunity Fraud**

Business opportunity or "work-at-home" schemes are also making their way onto the Internet. In *United States v. Shklowiski* (C.D. Cal. sentenced June 9, 2000), the defendants used the Internet to harvest e-mail addresses and send more than 50 million unsolicited e-mails ("spam") to offer people a "work-at-home" opportunity that promised tremendous returns in exchange for a \$35 "processing fee." Approximately 12,405 individual victims sent money to what they thought were various businesses, but in fact, were postal mailboxes. As part of the scheme, the defendants forged the e-mail headers in their "spam" to make it appear that the e-mails were coming from an Internet service provider, BigBear.Net. As a result of the header forgery, when approximately 100,000 recipients of the spam responded with complaints by e-mail, the unexpected large volume of e-mails caused BigBear.Net's computer file servers to crash or cause disruptions in their service to customers. BigBear.Net had to hire three temporary workers

for nearly six months to respond to the large numbers of complaints. (Ultimately, two defendants, after pleading guilty to conspiracy to commit mail and wire fraud, were sentenced to twenty seven months' imprisonment and restitution of \$104,000 to fraud victims, including BigBear.Net).

### **The Response to Internet Fraud**

As the case examples above indicate, more and more United States Attorneys' Offices are pursuing significant cases of Internet fraud. The cases being prosecuted tend to show that the criminal statutes that apply to other types of white collar crime – conspiracy, mail and wire fraud, credit card fraud, securities fraud, money laundering, and identity theft – are equally applicable to various forms of Internet fraud. In addition, a variety of existing sentencing guidelines enable federal prosecutors to seek higher sentences in appropriate cases of Internet fraud. These include enhancements for mass-marketing (USSG § 2F1.1(b)(3)), identity theft (USSG § 2F1.1(b)(5)(C)), conducting a substantial part of a scheme from outside the United States (USSG § 2F1.1(b)(6)(B)), large numbers of vulnerable victims (USSG § 3A1.1(b)(2)(B)), and use of a special skill (USSG 3B1.3; *compare* *United States v. Petersen*, 98 F.3d 502, 506-08 (9th Cir. 1996), *with* *United States v. Godman*, 223 F.3d 320, 322 (6th Cir. 2000)).

Nonetheless, the Department has a strong interest in continuing to enhance its capabilities to combat Internet fraud. To that end, in February 1999, the Department established an Internet Fraud Initiative. This Initiative, which the Fraud Section of the Criminal Division oversees, has provided a vehicle for improving coordination and cooperation on Internet fraud enforcement at all levels of law enforcement, through such means as:

- Training. Since 1999, the National Advocacy Center (NAC) has conducted specialized seminars on Internet fraud for more than 180 federal, state, and local prosecutors (including Assistant United States Attorneys (AUSAs from fifty three districts), FBI agents, local police, and even foreign prosecutors from five foreign countries. In addition, the NAC has

---

---

revised its basic Cybercrimes Seminar to include a specific track on Internet fraud, and the National Cybercrimes Training Partnership has included an Internet fraud training module in its cybercrimes training program.

- **Advice and Litigation.** The Fraud Section of the Department's Criminal Division, which oversees the Initiative, provides regular points of contact for federal prosecutors needing advice or information on Internet fraud cases, as well as a brief bank of relevant pleadings and materials. The Fraud Section also provides first-chair and second-chair prosecutors in particular Internet fraud cases.
- **Analysis and Referrals.** The IFCC now provides federal prosecutors with a national resource from which they can receive referrals of possible Internet fraud cases, or to which they can submit requests for queries and other assistance in identifying possible Internet fraud schemes. The IFCC's Website is located at [www.ifccfbi.gov](http://www.ifccfbi.gov). In addition, as a result of continuing cooperation between the Department and the FTC, the FTC has substantially improved its Consumer Sentinel database, which contains more than 300,000 consumer complaints about Internet fraud and other consumer frauds that prosecutors can search for leads and witness information.
- **Outreach and Prevention.** The Department has posted a set of Webpages on Internet fraud, [www.internetfraud.usdoj.gov](http://www.internetfraud.usdoj.gov), that contains information on the nature and types of fraud schemes, what the public should do to deal with Internet fraud, and how to report possible Internet fraud. In addition, as part of its response to identity theft the Department also has posted a set of informative Webpages on identity theft and fraud, [www.usdoj.gov/criminal/fraud/idtheft.html](http://www.usdoj.gov/criminal/fraud/idtheft.html). The Department also coordinates with other agencies to develop and support public education efforts directed at consumer protection matters relating to Internet fraud, such as identity theft.
- **International Coordination.** Through the work of the G-8's Senior Experts Group on

Transnational Organized Crime (the "Lyon Group"), the G-8 Ministers of Justice issued a communique in October, 1999, in which they declared their commitment to a comprehensive effort against Internet fraud that includes investigation, prosecution, and prevention. The Department continues to use the Lyon Group process to expand on existing investigative, prosecutive, and prevention efforts.

As the Internet continues to grow and adapt to changing circumstances, Internet fraud will also tend to grow and adapt, as criminals try to circumvent new fraud prevention measures and law enforcement capabilities for combating the problem. Law enforcement, at all levels of government, will need to continue devising and applying methods to investigate and prosecute Internet fraud criminals faster than criminals can adapt to those methods. ~

#### ABOUT THE AUTHOR

**Jonathan Rusch** is Special Counsel for Fraud Prevention in the Fraud Section of the Criminal Division. His responsibilities include coordination of the Internet Fraud Initiative, a Department-wide initiative established in 1999 to improve the Department's abilities to combat all forms of Internet fraud. He also serves as Chair of the interagency Telemarketing and Internet Fraud Working Group. Mr. Rusch is an Adjunct Professor of Law at Georgetown University Law Center, where he teaches courses on Global Cybercrime Law and International and Comparative Law of Cyberspace, and has written several law review articles on various aspects of cyberspace law. He received the Attorney General's Award for Distinguished Service in 1995. **a**

---

---

# Tracking a Computer Hacker

*Daniel A. Morris*  
*Assistant United States Attorney*  
*Computer and Telecommunications*  
*Coordinator*  
*District of Nebraska*

A report written near the start of the Information Age warned that America's computers were at risk from hackers. It said that computers that "control [our] power delivery, communications, aviation and financial services [and] store vital information, from medical records to business plans, to criminal records," were vulnerable from many sources, including deliberate attack. "The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." National Research Council, "Computers at Risk," 1991.

To see what computer hackers are doing today, take a look at [www.attrition.org](http://www.attrition.org). This is one of the places on the Internet where hackers receive "credit" for their attacks. If the operator of this website verifies that a computer system has been invaded, a "mirror" of the damage, often a defaced web page, is posted on the website along with a link to the undamaged website. More importantly to the person or group claiming credit, the online nickname of the responsible hacker (HaXoBuGz, databoy and HACKWEISER being examples) is included next to the published description of the intrusion. This fleeting notoriety is what motivates many hackers. Other hackers cause even greater damage and try to avoid notice, much less notoriety.

Information about some of the Department of Justice's successes in prosecuting hackers can be found on the Department's website at [www.cybercrime.gov](http://www.cybercrime.gov). This site includes manuals for searching and seizing computers, policy statements, useful background material, and press releases regarding hacker prosecutions. It is one of the first places prosecutors should go when called

upon to assist investigators looking into computer intrusions.

## **Hacker Tools Available Online**

Some websites on the Internet provide both novice and expert computer hackers with programs, sometimes called "exploits," needed to conduct attacks. These sites may provide services to computer security experts and even advise hackers that they should not use the posted exploits to hack into another computer. Anybody, including some very destructive people, can download the hacker tools or "scripts" coded by experienced hackers, along with instructions for their use. *See, e.g.*, <http://www.securityfocus.com> and its "bugtraq" service.

Hackers who find exploits on these websites may use them to do more than just deface webpages. Novices, sometimes referred to in hacker circles as "script-kiddies," who download hacker scripts may gain "root" access to a computer system, giving them the same power over a computer system as a trusted systems manager -- such as the power to create or delete files and e-mails and to modify security features.

Hackers who gain such unauthorized root access sometimes speak of this as "owning" the system they hack. If they want to cause damage they may do so immediately, or they may plant viruses or time bombs in a system. Sometimes they configure the system to work for them in later "denial of services" attacks on other computers.

Some websites that post hacker tools also post known fixes, or patches. They advise systems administrators and network operators to download and install these patches so their systems will no longer be vulnerable to the listed attacks. But hackers know that, with persistence and help from other readily available computer programs, they can find computer systems vulnerable to the listed exploits. Hackers frequently launch their attacks against these unprotected systems.

---

It is commonly believed that many systems operators do not share information when they are victimized by hackers. They don't contact law enforcement officers when their computer systems are invaded, preferring instead to fix the damage and take action to keep hackers from gaining access again -- with as little public attention as possible.

### **Protected Computers**

Federal law enforcement officers may be called in to track a hacker if the hacker gains unauthorized access to a Federal Government computer or to a computer system protected by federal law. Protected computers are any computer used in interstate or foreign commerce or communications, which includes any computer connected to the Internet. 18 U.S.C. § 1030(e)(2)(B).

Tracking a hacker may call for a combination of Internet research skills, subpoenas, court orders, search warrants, electronic surveillance and traditional investigative techniques. At least one Assistant United States Attorney (AUSA) in every district has been trained as a Computer and Telecommunications Coordinator (CTC) to assist law enforcement officers and other AUSAs in this effort. CTCs can obtain guidance from attorneys in the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS)(pronounced See-sips). CCIPS attorneys deal with these issues daily.

### **Clues of a Cybercrime**

Clues to the identity of a hacker often exist in cyberspace and in the real world if the investigator knows where to look.

Computer systems of interest to hackers usually keep track of all authorized and unauthorized access attempts. Records, called computer logs, provide useful and often critical clues that a trained agent or computer specialist can use as the starting point to trace the route taken from computer to computer through the worldwide web, to discover the one computer out of the millions in the world from which an intrusion was conducted.

All computers using the Internet are assigned a different numeric Internet Protocol (IP) address while online, similar to country, city, street, and number addresses for houses. Unless the hacker alters the victim's logs once he or she gains unauthorized access, the victim's logs should list the precise computer address from which unauthorized access was gained. That address may not be the hacker's own computer, but instead another computer that the hacker has hijacked or an account that he owns on a third party's computer, as discussed in more detail below.

Lookup tools are available online to identify the owner of the network through which an attack was launched. To see how this works, see [www.arin.net](http://www.arin.net), operated by the American Registry of Internet Numbers.

### **Obstacles to Identifying the Hacker**

Because of the make-up of the Internet, it is sometimes difficult for law enforcement officers to discover the identity of a hacker.

1. A hacker might hide or "spoof" his Internet Protocol (IP) address, or might intentionally bounce his communications through many intermediate computers scattered throughout the world before arriving at a target computer. The investigator must then identify all the bounce points to find the location of the hacker, but usually can only trace the hacker back one bounce point at a time. Subpoenas and court orders to each bounce point may be necessary to identify the hacker.

2. Some victims don't keep logs or don't discover a hacker's activities until it is too late to obtain records from the hacker's Internet Service Provider (ISP). A victim who has no record of the IP address of the computer from which unauthorized access was gained limits law enforcement officers to traditional investigative techniques, which alone may be inadequate to identify the hacker.

3. Some ISP's don't keep records or don't keep them long enough to be of help to law enforcement officers. As explained below, when the investigator determines the identity of an ISP from which records will be needed, the prosecutor should send a retention letter under 18 U.S.C.

---

§ 2703(f) requiring the ISP to preserve the records while a court order or other process is being obtained.

4. Some computer hackers alter the logs upon gaining unauthorized access, thereby hiding the evidence of their crimes.

5. Some leads go through foreign countries, not all of which consider hacking a crime. Treaties, conventions, and agreements are in place with some countries, and there are "24/7" contacts in dozens of countries around the world who can be contacted for help. When a lead points to a foreign country, the investigator should contact a CTC or CCIPS attorney.

### **Electronic Communications Privacy Act**

Some of the information investigators need to track a hacker might be readily available to the general public on the Internet. No special restrictions apply to an investigator's access to and use of such information – in the same way that information available in a public library can be used by investigators without special authorization. Common search engines such as [www.dogpile.com](http://www.dogpile.com), [www.lycos.com](http://www.lycos.com), [www.excite.com](http://www.excite.com), or [www.netscape.com](http://www.netscape.com) may be used to find information about a username or nickname of the person or group claiming credit for a computer intrusion.

Other information, such as the content of e-mails, is available to law enforcement officers only if they comply with the provisions of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2701-11. ECPA creates statutory rights for customers and subscribers of computer network service providers. The details of this Act are beyond the scope of this article, but an excellent guide to the Act is provided by CCIPS in print and on its webpage. *See* Computer Crime and Intellectual Property Section, Department of Justice, Prosecuting Intellectual Property Crimes Manual *available at* <http://www.cybercrime.gov>.

Section 2703 of ECPA provides investigators with five mechanisms for compelling an Internet Service Provider to disclose information that might be useful in an investigation of a hacker.

The mechanisms, in ascending order of the threshold showing required, are described below:

1. Subpoenas can be used by an investigator to obtain basic subscriber information from an Internet Service Provider, including "the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of such service and the types of service the subscriber or customer utilized." 18 U.S.C. § 2703(c)(1)(C).

2. Subpoenas also can be used to obtain opened e-mails, but only under certain conditions relating to notice to the subscriber. *See* 18 U.S.C. § 2703(b)(1)(B). Notice may be delayed under Section 2705 for successive 90-day periods. Subpoenas may be issued for e-mails that have been opened, but a search warrant is generally needed for unopened e-mails.

3. Court orders under 18 U.S.C. § 2703(d) can be obtained by investigators for account logs and transactional records. Such orders are available if the agent can provide "articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.*

The government must offer facts, rather than conclusory statements, in an application for a 2703(d) order. A one to three-page factual summary usually is sufficient for this purpose. The standard for issuing such an order is not as high as for a search warrant.

4. Investigators who obtain a court order under 18 U.S.C. § 2703(d) can obtain the full contents of a subscriber's account (except for unopened e-mail stored with an ISP for 180 days or less and voice-mail), if the order complies with a notice provision in the statute. 18 U.S.C. § 2703(b)(1)(B)(ii) and (b)(2). Notice to the subscriber can be delayed for up to ninety days when notice would seriously jeopardize the investigation. 18 U.S.C. § 2705(a).

5. Search warrants obtained under Rule 41 of the Federal Rules of Criminal Procedure or an equivalent state warrant can be used to obtain the

---

full contents of an account, except for voice-mail in electronic storage (which requires a Title III order). The ECPA does not require notification to the subscriber when the government obtains information from a provider using a search warrant.

Warrants for information regarding evidence of a computer intrusion are usually obtained like all other search warrants but are served like subpoenas. That is, the agents serving the warrants on an ISP ordinarily do not search through the providers computers. Instead, they serve the warrants on the provider and the provider produces the material described in it.

### **Voluntary Disclosures**

Investigators can obtain the contents of a hacker's communications stored on the victim system without first obtaining an order or a subpoena, pursuant to 18 U.S.C. § 2702(b). For example, a hacker's victim may voluntarily disclose the contents of internal e-mails relevant to the attack.

Voluntary disclosure by a provider whose services are available to the public is forbidden unless certain exceptions apply. These exceptions include disclosures "incident to the rendition of the service or the protection of the rights of property of the provider of the service." 18 U.S.C. § 2702(b)(5). *See* 18 U.S.C. §§ 2702(b)(1)-(4),(6)(A)-(B) for other exceptions.

### **Early Communication with ISPs**

Investigators should contact a network service provider as soon as possible to request that the ISP retain records that may be relevant to an investigation. This is often done through the AUSA who is assisting the agent in the investigation. The AUSA should send a letter to the ISP directing it to freeze stored records, communications, and other evidence pending the issuance of a court order or other process. 18 U.S.C. § 2703(f).

If the investigator wants to be sure the ISP does not disclose that the ISP has been asked for information pursuant to a subpoena, order or warrant, an order not to disclose can be obtained under 18 U.S.C. § 2705(b).

### **Electronic Surveillance**

Investigators tracking down hackers often want to monitor a hacker as he breaks into a victim's computer system. The two basic statutes governing real-time electronic surveillance in other federal criminal investigations also apply in this context.

The first is the wiretap statute, 18 U.S.C. §§ 2510-22, generally known as a Title III order.

The second statute relates to pen registers and trap and trace devices. 18 U.S.C. §§ 3121-27.

DOJ's manual for obtaining evidence of this type, says "In general, the Pen/Trap statute regulates the collection of addressing information for wire and electronic communications. Title III regulates the collection of actual content for wire and electronic communications." Computer Crime and Intellectual Property Section, Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigation 71 (2001) *available at* <http://www.cybercrime.gov/searchmanual.pdf>.

A warrant is suggested, at a minimum, when an investigator wants to obtain access to opened voice mail, but the requirements of Title III apply if the investigator wants access to voice mail messages not yet retrieved by a subscriber or customer.

### **Nationwide Scope of Tools Used in Hacker Investigations**

18 U.S.C. § 2703(d) orders are nationwide in scope, as are subpoenas. Other tools used in hacker investigations contain express geographic limitations. Search warrants under Fed.R. Crim.P. 41(a), Title III orders permitting the interception of communications, and 18 U.S.C. § 3123(a) orders authorizing the installation of pen registers and trap and trace devices all apply only within the jurisdiction of the court.

### **Search Warrants**

Search warrants may be obtained to gain access to the premises where the hacker is believed to have evidence of the crime. Such evidence would include the computer used to commit the crime, as well as the software used to

---

---

gain unauthorized access and other evidence of the crime. Suggested language for a search warrant for evidence of this type is available in the online manual prepared by CCIPS.

### **Analyzing Evidence from a Hacker's Computer**

A seized computer may be examined by a forensic computer examiner to determine what evidence of the crime exists on the computer. The court order should specifically authorize this search. Many federal agencies have trained personnel on staff who are able to prepare a mirror image of everything in the memory of a seized computer – often including the memory of things the computer owner thought had been erased. The computer examiner will prepare a detailed report regarding the information on the computer and should be able to testify as an expert at trial.

### **The Use of Traditional Investigative Techniques**

Information obtained through the methods described above may reveal the subscriber or customer whose computer was used to conduct an intrusion. If it does, traditional investigative techniques may then be needed to determine who actually used the identified computer to commit the crime.

Due to the anonymity provided by the Internet, a suspected hacker may claim that someone else used his computer and assumed his identity at the time of the attack. It may be difficult to prove otherwise. For example, in a case charged in the District of Nebraska, the identity of the suspected hacker who defaced a newspaper's webpage by adding a bogus story was obtained even though computer logs showing the IP address of the hacker came to a dead-end because the hacker had used an ISP that provided anonymous access to the Internet. *United States v. Lynch*, 8:00CR344 (D. Neb. indictment filed Dec. 14, 2000). The now-defunct [www.worldspy.com](http://www.worldspy.com), kept no records of its users. Similar services still exist, such as [www.anonymizer.com](http://www.anonymizer.com).

In the Nebraska case, calls to people in the community with the same last name as the person who was the subject of the unflattering article led

authorities to the subject of the article, and that person led the FBI to the suspected hacker. Using tools available to obtain evidence of cybercrimes, including traditional investigative techniques such as this, federal law enforcement officers will continue to track down hackers and bring them to justice.

### **ABOUT THE AUTHOR**

**Daniel A. Morris** is an Assistant United States Attorney (AUSA) in the District of Nebraska and is the Computer and Telecommunications Coordinator (CTC).

Mr. Morris has been an AUSA since 1987. Before that he was a Senior Corporate Counsel for the Mutual of Omaha Companies.

Mr. Morris is the author of two books, the *Nebraska Trial Handbook* and *Federal Tort Claims*, both published by West Publishing Company. He has published articles in the *Creighton Law Review* and for several years, was a regular contributor to *Case and Comment*, a magazine for lawyers.

Mr. Morris thanks CCIPS attorney Richard Downing for his comments and suggestions regarding this article and also thanks Patrick DeWall, a law clerk for the District of Nebraska for his assistance. [daniel.morris@usdoj.gov](mailto:daniel.morris@usdoj.gov)

---

---

# Tracing in Internet Fraud Cases: PairGain and NEI Webworld

*Christopher M.E. Painter*  
*Deputy Chief, Computer Crime*  
*and Intellectual Property Section*

Fraud, including stock manipulation and the full panoply of other deceitful schemes, has found a comfortable home on the Internet. Many of these crimes are simply age-old schemes being committed over a new medium – so called old wine in new bottles. Others, like Internet auction fraud or the easy dissemination of digital copyrighted works, are novel and have been spawned by the new technology. In either case, crimes committed over the Internet pose special challenges for law enforcement.

Investigative agents and prosecutors must be technically savvy and react very quickly in tracking down Internet criminal perpetrators. Unlike traditional fraud cases that might have been investigated for many months or even years, crimes committed on the Internet must be tracked promptly or the digital trail will run cold. Indeed, many Internet Service Providers (ISPs), to whom investigators must go to get computer logging information, email and other vital pieces of evidence, retain such logging and other information for a very short period – in some cases less than a week. Because these cases are fast-moving and special legal process is needed to obtain much of the digital evidence successful investigation requires, to an unprecedented degree, close teamwork between the investigators and the prosecutors. The old model of agents conducting the investigation with little input from the prosecutor until an investigative report is generated simply does not work when an investigation is highly reactive and takes place in days rather than over a protracted period. Also, the inherently technical nature of the Internet and the anonymity it often affords criminals requires investigators to possess unprecedented technical sophistication. Technically trained agents who know how to trace illegal conduct over the

Internet and who can effectively discuss the evidence they need with Internet communications providers are essential. Technically and legally trained prosecutors who can prepare the correct legal process and guide the investigation are also indispensable. Moreover, because these cases have no simple geographic boundaries, with victims spread around the country and facilities that often span many states and foreign countries, agents and prosecutors must cooperate with their counterparts in many jurisdictions. Nearly seven years ago, the Computer Crime and Intellectual Property Section in the Department of Justice set up a network of Computer and Telecommunications Coordinators (“CTCs”) in every United States Attorney’s Office (USAO) to facilitate this kind of coordination and cooperation for high tech crimes. This group of technically-trained Assistant United States Attorneys (AUSA) provides a network response to what are necessarily network crimes. Even where the CTC is not personally involved in a particular matter, he or she serves as a point of contact and expertise. Finally, traditional investigative work should not be ignored. Cases involving the Internet always combine cyber-investigative methods with traditional gumshoe techniques. Indeed, unlike many hacking cases, Internet fraud cases almost always involve money. Despite the Internet’s increasing anonymity, following the money trail is an age-old investigative method that still yields high dividends.

In order to illustrate some of these principles, and to highlight some of the information that can be obtained in these investigations, I will briefly discuss two Internet stock manipulation cases that I prosecuted with agents of the Federal Bureau of Investigation (FBI) in Los Angeles. The first, *United States v. Hoke* (PairGain), CR 99-441 (C.D. Cal. indictment filed April 30, 1999), illustrates how a wrongdoer can be traced over the Internet despite the seeming anonymity it offers. The second, *United States v. Aziz-Golshani*, CR

---

00-7 (C.D. Cal. indictment filed January 4, 2000) illustrates the combination of traditional and cyber-investigative methods. Both show the need for speed and teamwork when the Internet is involved.

In the morning of April 7, 1999, users of Internet bulletin boards hosted by Yahoo! Finance and other companies devoted to the discussion of a company named PairGain saw a message from an individual identifying herself as Stacey Lawson of Knoxville Tennessee. The message reported that PairGain, a telecommunications equipment company located in California, would be purchased for 1.35 billion dollars by an Israeli company. The message contained a link to what it stated was the Bloomberg News story reporting the impending merger. Other messages, purportedly from other individuals, also discussed the news in excited terms advocating that readers purchase the stock immediately. When users clicked on the link in the first message they were taken to what appeared to be a legitimate Bloomberg News web page containing a detailed story on the merger. Although the page looked exactly like a real Bloomberg page, even to the point of including other links that took the reader back to the real Bloomberg service, it was, in fact, bogus and the story of the merger was false. Because the message was reported early east coast time, no one could reach PairGain for comment because of the time difference. No one could reach the Israeli company because it was an Israeli holiday. In just two hours, the false news triggered a buying spree – PairGain stock rose over 31% on NASDAQ with ten times its normal volume. When the hoax was exposed the stock fell causing thousands of victims to lose substantial amounts of money.

Almost immediately after the hoax was discovered, the USAO in Los Angeles and the Los Angeles division of the FBI began to investigate. The traditional side of the investigation, coordinated with the Securities and Exchange Commission (SEC), looked for unusual trading activity in PairGain stock to see who stood to profit from the hoax. This proved to be a dead end. Meanwhile, the cyber side of the investigation started examining the electronic

footprints. In less than a week, the perpetrator was tracked and arrested.

The cyber investigation focused on messages posted to Yahoo! and on the bogus Bloomberg web page. The Yahoo! messages were unrevealing, containing screen names such as Stacey LTN that were clearly false. Examination of the bogus web page revealed it was hosted on an Internet web hosting service named Angelfire. Angelfire is a free service that allows users to create their own web pages asking only that they provide subscriber information and an email account so that a password can be emailed to the user. Subscriber information, usually obtained by a subpoena, was unhelpful. Angelfire does not validate this information and the user provided obviously false information – listing his first name as “headlines” and last name as “99.” The email account provided to Angelfire was a Hotmail account. Hotmail is another free service that does not validate user information. Not surprisingly, the information provided by the target to Hotmail was also false. The perpetrator had tried to cover his tracks by falsifying his identity and, at first blush, had apparently succeeded. Nevertheless, because of the technical expertise of the agent and the prosecutor, additional material was sought from Angelfire and Hotmail that was a gold mine of evidence. Both Hotmail and Angelfire maintained logging information pertaining to the use of their services. This information is ordinarily obtained using a specialized court order under 18 U.S.C. § 2703(d). This court order is also called an articulable facts order because it must be based on articulable facts that the evidence is relevant to a criminal investigation. *See generally*, Computer Crime and Intellectual Property Section, United States Department of Justice, Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations (2000) *available at* <http://www.cybercrime.gov/searchmanual.pdf>. (for further discussion of § 2703 and other legal requirements for obtaining electronic evidence).

Unbeknownst to the target, Angelfire logged the Internet Protocol (“IP”) number of the computer accessing it every time the target logged on to Angelfire to create or modify the bogus Bloomberg page. An IP number is a unique

---

identifier for every computer connected to the Internet. An IP number can be either static or dynamic. A static IP is usually connected with a computer that is always on and directly connected to the Internet such as company or university computers. A dynamic IP is usually assigned to an Internet Service Provider (“ISP”) such as America Online or Mindspring. In the case of a dynamic IP, the IP number is assigned to a user when he or she dials into the ISP through a modem and is unique to that user for that particular session. When the user signs off the IP number is assigned by the ISP to a new user. Angelfire logs showed that the target accessed his account 11 times in the month and one half prior to the date the false page was sprung on the Internet. These accesses came from several different IP numbers. By looking these numbers up in publically available listing services, it was determined that the numbers corresponded to computers at PairGain (static IP numbers) and at Mindspring, a large ISP (dynamic numbers). Hotmail also maintained logs that also indicated accesses to the Hotmail account used to set up the Angelfire account. Again the logs showed accesses from PairGain and Mindspring.

For a number of reasons, including uncertainty as to whether the target was a PairGain employee, possibly in a position to destroy data on learning that law enforcement was on his trail, the company was not initially approached. Rather, a careful list of IP numbers, dates, and exact times was presented to Mindspring with a request (pursuant to subpoena) to identify the user account who made the accesses to Angelfire and Hotmail. The account was identified in every instance as the “ghoke” account. This did not necessarily mean that the owner of this account was responsible because the account could have been hacked or used without the user’s permission. Nevertheless, Mindspring had additional logging information called “radius logs” that, on each occasion, identified the phone number used to dial into Mindspring’s service. These caller-ID type logs indicated that the calls were placed from a phone belonging to Gary Hoke, a PairGain employee in a Raleigh, North Carolina branch office, and the owner of the “ghoke” account on Mindspring. This, of course, provided probable cause to believe that evidence

of the crime was at Hoke’s residence. Through close cooperation of FBI agents in Los Angeles and Raleigh and AUSAs in those jurisdictions, a search warrant was obtained. The search turned up a laptop that contained portions of the fake Bloomberg web page despite the defendant’s attempts to erase the data following the news reports of his misdeeds. The defendant, Gary Hoke, later pled guilty to securities fraud.

Although Hoke intended to trade in PairGain stock, he got “cold feet” and never capitalized on the hysteria he created. Accordingly, traditional investigative methods alone would have never succeeded. If the investigation did not move swiftly the cyber trail would also have been unavailing. Although Angelfire, Hotmail, and Mindspring all had very useful logging information, that information is only held for a short time. Title 18 U.S.C. § 2703(f) provides that such services can be requested to freeze relevant logging and other information for a period of ninety days (extendable for another ninety days), while legal process is obtained. Yet, even using this section, unless the logs are obtained promptly, the next link in the chain (here Mindspring) might not be discovered until after the relevant logs are no longer available. This emphasizes the need for the prosecutor and agents to work as a team and to know what types of electronic evidence might exist and how to obtain that evidence.

Another Internet stock manipulation case illustrates the value of combining cyber and traditional investigative methods. Following Gary Hoke’s arrest, many people were surprised by the logging information that was available. Some mused that a criminal could evade apprehension if he used computers that were difficult to trace to a particular individual, such as the public computers at a library or Internet café. This is precisely what happened in the investigation of the manipulation of NEI Webworld stock. In that case, the defendants bought a large volume of a bulletin board stock that traded for between thirteen and fifteen cents during a two week period. After the market closed on Friday, they sent out hundreds of messages on hundreds of Internet bulletin boards reporting a merger and the promise of huge profits. On Monday, based on orders made by those who believed the fake postings over the

---

---

weekend, the stock rose to fifteen *dollars* a share before plummeting to less than a quarter. Again the FBI and SEC rapidly began to trace the Internet postings. This time, however, the trail led to public computers at a University of California at Los Angeles library. Now traditional techniques made the difference. Following the money trail revealed that only four individuals bought the stock in the week preceding the scam. All, conveniently, sold their holdings on Monday reaping huge profits. A security camera video from outside the library showed the individuals entering the library during the period the fraudulent posts were made. The FBI also approached one of these individuals, then a UCLA student, and he agreed to cooperate and to wear a wire. That led to a number of incriminating statements cementing securities fraud charges and eventual guilty pleas against Arash Aziz-Golshani and Hootan Maleded.

Like PairGain, speed and coordination (both between agents and prosecutors and between criminal authorities and the SEC) were keys to a successful outcome. Knowledge of cyber tracking methods also played an important role both in the investigation and in making sense of the false postings that constituted the bulk of the evidence. Accordingly, both prosecutors and agents interested in doing these cases should seek out specialized training. The National Advocacy Center offers several basic computer crime courses each year that provide a good foundation in the law and technology of network investigations. The CCIPS web site, [www.cybercrime.gov](http://www.cybercrime.gov), contains a wealth of information including a comprehensive manual on obtaining electronic evidence (soon to be published by the Office of Legal Education). Also, AUSAs should avail themselves of the expertise of the CTCs in their offices. Armed with this expertise, Internet cases, while challenging, are rewarding and send a strong deterrent message that law enforcement is on the Internet beat.

## ABOUT THE AUTHOR

**Christopher M.E. Painter** is a Deputy Chief of the Computer Crime and Intellectual Property Section at the Department of Justice. From 1991 to March 2000, Mr. Painter was a criminal prosecutor in the U.S. Attorney's Office for the Central District of California (Los Angeles). Since taking that post, Mr. Painter specialized in the investigation and prosecution of high-tech, intellectual property and computer crimes and served as a Computer Crime and Internet Fraud Coordinator for his office.

Mr. Painter has investigated and prosecuted some of the most significant and high profile high-tech cases in the country, including the prosecution of notorious computer hacker Kevin Mitnick, the prosecution of the first Internet stock manipulation case involving the posting of a bogus Bloomberg News page falsely reporting the sale of a company called PairGain that caused its stock to soar, prosecution of another internet stock manipulation case, involving former and present UCLA students who hyped stocks on Yahoo by posting false spam messages, and the prosecution of one of the first Internet auction fraud cases. Mr. Painter co-chairs an ABA subcommittee concerning high-tech crimes and serves on several Department of Justice and interagency working groups relating to computer and Internet hackers, Internet fraud investigations and prosecutions, electronic evidence, intellectual property crimes, and thefts of trade secrets. He has frequently lectured to private groups and at the National Advocacy Center, appeared on 60 Minutes, CNN, CBS Morning News, the BBC, and has testified before Congress concerning computer crime issues. 

---

---

# Communications Assistance for Law Enforcement Act (CALEA)

*CALEA Implementation Section  
Federal Bureau of Investigation*

## Introduction

Electronic surveillance is one of the most valuable tools in law enforcement's crime fighting arsenal. In many instances, criminal activity has been either thwarted, or, if crimes have been committed, the criminals have been apprehended as a result of lawfully-authorized electronic surveillance.

The use of lawfully-authorized electronic surveillance continues to increase in importance to law enforcement as telecommunications systems become cornerstones of everyday life. Dependence on telecommunications for business and personal use has increased dramatically, computers and data services have become increasingly important to consumers, and the nation has become enthralled with mobile communications.

Three primary techniques of lawfully-authorized electronic surveillance are available to law enforcement: pen registers, trap and trace devices, and content interceptions. Pen registers and trap and trace devices, which account for the vast majority of lawfully-authorized surveillance attempts, record/decode various types of dialing and signaling information utilized in processing and routing the communication, such as the signals that identify the numbers dialed (i.e., outgoing) or the originating (i.e., incoming) number of a telephone communication. A third and more comprehensive form of lawfully-authorized electronic surveillance includes not only the acquisition of call-identifying, or dialed number information, but also the interception of communications content.

Although lawfully-authorized electronic surveillance is crucial to effective law enforcement, it is used sparingly. This is

particularly true with respect to the interception of communications content. The federal government, District of Columbia, Virgin Islands, and forty-five states allow the use of this technique, but only in the investigation of felony offenses, such as kidnapping, extortion, murder, illegal drug trafficking, organized crime, terrorism, and national security matters, and only when other investigative techniques, either can not provide the needed information or would be too dangerous.

## I. Legal Origins of Electronic Surveillance

Passage of the Communications Assistance for Law Enforcement Act (CALEA) 1994 Pub. L. No. 103-414, 108 Stat. 4279, was not without precedent; it was a logical and necessary development of the nation's electronic surveillance laws.

The modern legal framework for electronic surveillance arises out of the Supreme Court's landmark decision in *Katz v. United States*, 389 U.S. 347 (1967). Prior to *Katz*, the Supreme Court had regarded wiretapping as outside the scope of the Fourth Amendment's restrictions on unreasonable searches and seizures. See *Olmstead v. United States*, 277 U.S. 438 (1928). In *Katz*, however, the Supreme Court reversed its prior position and held for the first time that Fourth Amendment protections do apply to government interception of telephone conversations.

A year after the *Katz* decision, and after a failed attempt to address wiretapping through amendments to the Communications Act of 1934, Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968. Section 605 of the Communications Act of 1934 was amended to provide that "no person not being authorized by the sender shall intercept any communication and divulge or publish [its] existence, contents . . . or meaning." By 1968, the provisions of the Act dealing with wiretapping had become so muddled

---

by inconsistent interpretations of federal and state courts that Congress intervened. *See* Pub. L. No. 90-351, 82 Stat. 212.

Title III of the Omnibus Act created the foundation for communications privacy and electronic surveillance law. The Omnibus Act not only established a judicial process by which law enforcement officials could obtain lawful authorization to conduct electronic surveillance, but also prohibited the use of electronic surveillance by private individuals. A subsequent amendment to Title III also required telecommunications carriers to “furnish [law enforcement] . . . all information, facilities, and technical assistance necessary to accomplish [an] interception.” 18 U.S.C. § 2518[4].

In response to continued advances in telecommunications technology, Congress expanded the protections of Title III by enacting the Electronic Communications Privacy Act (ECPA) 1986 Pub. L. No. 99-508, 100 Stat. 1848. Among the ECPA amendments to Title III were requirements that: (1) interceptions be conducted unobtrusively and with a minimum of interference with the services of the person whose communications are being intercepted; and (2) the interception be conducted in such a way as to minimize access to communications not otherwise authorized to be intercepted. ECPA also expanded electronic surveillance authority to include telecommunications technologies and services such as electronic mail, cellular telephones, and paging devices.

Following the enactment of ECPA, advancements in telecommunications technology continued to challenge and, in some cases, thwart law enforcement’s electronic surveillance capability. What was once a simple matter of attaching wires to terminal posts now either required expert assistance from telecommunications service providers or was impossible altogether.

Although Title III required telecommunications carriers to provide “any assistance necessary to accomplish an electronic interception,” 18.U.S.C. § 2518[4], the question of whether telecommunications carriers had an obligation to design their networks such that they

did not impede a lawfully-authorized interception had not been decided.

In October 1994, at the request of the nation’s law enforcement community, Congress responded to this dilemma by enacting CALEA, which clarified the scope of a carrier’s duty in effecting lawfully-authorized electronic surveillance.

## **II. Communications Assistance for Law Enforcement Act**

Although telecommunications carriers have been required, since 1970, to cooperate with law enforcement personnel in conducting lawfully-authorized electronic surveillance, CALEA for the first time requires telecommunications carriers to modify the design of their equipment, facilities, and services to ensure that lawfully-authorized electronic surveillance can actually be performed. CALEA also imposes certain responsibilities on the Attorney General of the United States, the Federal Communications Commission (FCC), telecommunications equipment manufacturers, and telecommunications support services providers. A brief description of the roles and responsibilities of each is provided below.

### **A. Attorney General of the United States**

Congress assigned the Attorney General of the United States a key role in the implementation of CALEA, the most important being that of chief integrator and spokesperson for the law enforcement community. The responsibilities of the Attorney General include, but are not limited to:

- Consulting with industry associations, standard-setting organizations, representatives of users, and state utility commissions to facilitate implementation of the assistance capability requirements;
- Providing telecommunications carriers, telecommunications industry associations, and standard-setting organizations with an estimate of the number of interceptions, pen registers, and trap and trace devices that government agencies may conduct;
- Establishing regulations to facilitate timely and cost-efficient reimbursement to

---

---

telecommunications carriers as authorized under CALEA;

- Allocating funds appropriated for reimbursement in a manner consistent with law enforcement priorities; and
- Reporting to Congress, annually, the total amount of payments made to telecommunications carriers during the preceding year, and the projected expenditures for the current year.

#### **B. Federal Bureau of Investigation**

On February 24, 1995, the Attorney General delegated management and administrative responsibilities for CALEA to the Federal Bureau of Investigation (FBI) 28 C.F.R. § 0.85 (1995). The FBI, in turn, created the CALEA Implementation Section (CIS), which works with the telecommunications industry and the law enforcement community to facilitate effective and industry-wide implementation of CALEA.

#### **C. Federal Communications Commission**

Consistent with the FCC's duty to regulate the use of wire and radio communications, Congress assigned specific CALEA responsibilities to the FCC. These include, but are not limited to:

- Determining which entities should be considered telecommunications carriers for purposes of CALEA;
- Establishing systems security and integrity regulations for carrier administration of interceptions;
- Establishing technical requirements or standards for compliance with the assistance capability requirements of CALEA if industry associations or standard-setting organizations fail to issue technical requirements, or if a government agency or any other person believes that industry-adopted standards are deficient;
- Reviewing reasonably achievable petitions regarding compliance with the assistance capability requirements; and
- Reviewing petitions for extension of the capability compliance date.

CALEA also amends the Communications Act of 1934 to provide that the FCC "shall prescribe such rules as are necessary to implement [CALEA]" 47 U.S.C. § 229.

#### **D. Telecommunications Carriers**

Telecommunications carriers must ensure that equipment, facilities, or services that provide customers the ability to originate, terminate, or direct communications meet the following assistance capability requirements:

- Expedient isolation and interception of communications content;
- Expedient isolation and access to call-identifying information;
- Delivery of communications content and call-identifying information; and
- Unobtrusive interception and access to call-identifying information and protection of the privacy and security of communications not authorized to be intercepted.

#### **E. Equipment Manufacturers and Support Service Providers**

Congress also recognized that without the assistance of manufacturers of telecommunications equipment and support service providers, carriers would be unable to comply with CALEA. To that end, it imposed an affirmative duty on manufacturers of telecommunications equipment and support service providers to make available all features or modifications necessary to meet the assistance capability requirements of CALEA.

### **III. Legal Provisions of CALEA**

The CALEA statute consists of the following main sections:

#### **A. Section 102**

Section 102 defines key terms and phrases, such as call-identifying information, information services, and telecommunications carrier. Of the terms defined in section 102, telecommunications carrier required further clarification by the FCC. Specifically, the FCC addressed whether certain

---

---

telecommunications carriers are subject to CALEA's assistance capability requirements.

CALEA requires that all telecommunications carriers' equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of meeting specific assistance capability requirements. The Act defines such carriers as:

1. person[s] or entit[ies] engaged in the transmission or switching of wire or electronic communications as a common carrier for hire; and
2. includes-
  - a. person[s] or entit[ies] engaged in providing commercial mobile service (as defined in 47 U.S.C. § 332(d)); or
  - b. person[s] or entit[ies] engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this title; but
3. does not include-
  - a. persons or entities insofar as they are engaged in providing information services; and
  - b. any class or category of telecommunications carriers that the FCC exempts by rule after consultation with the Attorney General.

On August 31, 1999, the FCC released a Report and Order clarifying which entities and services are subject to the assistance capability requirements of CALEA. The following list provides illustrative examples of the *types* of entities determined by the FCC to be

telecommunications carriers for purposes of CALEA:

- All entities previously classified as common carriers;
- Cable operators and electric or other utilities to the extent that they offer telecommunications services for hire to the public;
- Commercial mobile radio service (CMRS) providers, including industrial and business radio services licensees, specialized mobile radio (SMR) providers, 220 megahertz (MHZ) service licensees, to the extent that such services consist of interconnected services offered to the public;
- Resellers, to the extent that they actually own facilities; and
- Entities that provide calling features, such as call forwarding, call waiting, three-way calling, and speed dialing.

Private mobile radio service (PMRS) operators and pay telephone providers were excluded from the list of carriers subject to CALEA. However, if a PMRS operator uses its facilities to offer interconnected service for profit to the public, or to a substantial portion of the public, that service qualifies as CMRS, and is therefore subject to CALEA.

The FCC also clarified that where facilities are used solely to provide an information service (IS), whether offered by an exclusive-IS provider or by a common carrier that has established a dedicated IS system apart from its telecommunications system, such facilities *are not* subject to CALEA. These include messaging and on-line services such as Prodigy and America Online. By contrast, facilities used to provide both telecommunications and information services (i.e., joint-use facilities) are subject to CALEA in order to ensure law enforcement's ability to access the telecommunications services portion of joint-use facilities.

#### **B. Section 103**

Section 103 of CALEA establishes four assistance capability requirements that telecommunications carriers are required to meet

---

---

in connection with services or facilities, that provide customers the ability to originate, terminate, or direct communications. They are:

1. Interception of Communications Content

Telecommunications carriers must ensure that they are capable of expeditiously isolating, and enabling the government to intercept pursuant to appropriate legal authorization, all wire and electronic communications to or from a particular subscriber within that carrier's network.

2. Access to Call-identifying Information

Telecommunications carriers must ensure that they are capable of expeditiously isolating, and enabling the government to access pursuant to appropriate legal authorization, all call-identifying information reasonably available to the carrier. Such information, however, if acquired solely through pen registers or trap and trace devices, does not include information that may disclose the physical location of the subscriber, except to the extent that location can be determined by the telephone number.

Section 102 of CALEA defines call-identifying information as ". . . dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier."

3. Delivery of Communications Content and Call-identifying Information

Telecommunications carriers must ensure that they are capable of delivering intercepted communications and call-identifying information to a location specified by the government, other than the carrier's premises. The information must be made available to the government in a format that can be transmitted over communications channels and either translated or converted into useable form.

4. Protection of Privacy and Security of Communications

Telecommunications carriers must ensure that they are capable of conducting interceptions and providing access to call-identifying information

unobtrusively. Carriers must also protect the privacy and security of communications and call-identifying information not authorized to be intercepted, as well as information about the government's interception of call content and access to call-identifying information. The requirement that interceptions be conducted in a manner that will minimize the interception of unauthorized communications was intended to avoid improper intrusion on rights of privacy.

**C. Section 104**

Section 104 of CALEA requires the Attorney General to provide notice of the actual and maximum "number of communications interceptions, pen registers, and trap and trace devices . . . that the Attorney General estimates" government agencies may "conduct and use simultaneously." Section 104 also requires that the Attorney General publish in the *Federal Register* the capacity notices "after consulting with State and local law enforcement agencies, telecommunications carriers, providers of telecommunications support services, and manufacturers of telecommunications equipment." In addition, section 104 mandates that the Attorney General publish capacity notices after notice and comment.

Section 104 consists of five subsections:

1. Notice of Actual and Maximum Capacity

The FBI began the process of implementing section 104 by publishing on October 16, 1995, the Initial Notice of Capacity in the *Federal Register*. Implementation of the Communications Assistance for Law Enforcement Act, 60 Fed. Reg. 53,643 (Oct. 16, 1995). On January 14, 1997, the Second Notice of Capacity was published. Implementation of Section 104 of the Communications Assistance for Law Enforcement Act, 62 Fed. Reg. 1902 (Jan. 14, 1997). A Final Notice of Capacity was published on March 12, 1998. Implementation of Section 104 of the Communications Assistance for Law Enforcement Act, 63 Fed. Reg. 53, 643 (Mar. 12, 1998).

The Final Notice of Capacity adopted capacity requirements for telecommunications services that law enforcement viewed as its highest priorities in implementing lawfully-

---

authorized electronic surveillance: wireline local exchange service, cellular service, and broadband PCS. Capacity requirements for wireline local exchange service providers are based on the geographic boundaries of a county, whereas the capacity requirements for cellular and broadband PCS providers is based on established market service areas as defined by licenses granted by the FCC.

The Final Notice of Capacity provided that telecommunications services other than wireline local exchange service, cellular, and broadband PCS would be addressed in future notices of capacity. As a continuation of the capacity process, the FBI issued a Notice of Inquiry, which gave interested parties an opportunity to provide input to the FBI as it develops law enforcement's capacity requirements for services other than wireline local exchange, cellular, and broadband PCS. A Further Notice of Inquiry was published to narrow the scope of the second phase to capacity requirements for paging, mobile satellite services, and specialized and enhanced specialized mobile radio.

## 2. Compliance

Subsection (b) of section 104 addresses carrier compliance with published capacity notices. It requires that telecommunications carriers ensure, within three years after publication of the notices or within four years of enactment, whichever is greater, that their systems are equipped with sufficient "actual" capacity and capable of "expeditiously" expanding to accommodate any necessary increases. Based on the publication date of the Final Notice of Capacity, telecommunications carriers had until March 12, 2001, to comply with the requirements. Because capacity requirements for telecommunications carriers other than wireline local exchange, cellular, and broadband PCS have not been published, a compliance date has not been established.

## 3. Notice of Increased Maximum Capacity Requirements

Section 104(c) states that notices of increased maximum capacity are to be published in the *Federal Register* by the Attorney General.

Similar to the actual and maximum capacity requirements, carriers have three years after the notice has been published to comply with the requirements. However, the Attorney General may specify a longer compliance period.

## 4. Carrier Statements

Within 180 days after the publication of the Final Notice of Capacity, section 104(d) requires that a telecommunications carrier submit a statement identifying all systems or services incapable of meeting the published capacity requirements. Telecommunications carriers had until September 8, 1998, to submit their carrier statement. The information obtained from the carrier statements will be used, in conjunction with law enforcement priorities and other factors, to determine which carriers may be eligible for capacity-related reimbursement.

## 5. Reimbursement

Section 104(e) provides a capacity "safe harbor" for telecommunications carriers who meet the following requirements. First, the carrier must have submitted a carrier statement pursuant to section 104(d). The Attorney General may, subject to the availability of appropriations, agree to reimburse a telecommunications carrier for costs directly associated with modifications to attain the capacity requirements, and the cost must be reasonable under section 109(e).

## D. Section 105

Section 105 of CALEA seeks to ensure systems security and integrity by requiring that a "telecommunications carrier ensure any interceptions of communications or access to call-identifying information . . . can be activated only in accordance with a court order or other lawful authorization and . . . in accordance with the regulations prescribed by the Commission." 47 U.S.C. § 1004.

On March 15, 1999, the FCC published a Report and Order, which promulgated systems security and integrity regulations that carriers must follow to comply with section 105 of CALEA. Implementation of the Communications Assistance for Law Enforcement Act, 64 Fed. Reg. 14,834 (Mar. 29 1999). Specifically, the

---

---

FCC addressed policies and procedures for employee supervision and control, record keeping requirements, the submission and review of carrier policies and procedures, and penalties for violation of carrier policies and Commission rules.

#### **E. Section 106**

Section 106 requires that telecommunications carriers consult with equipment manufacturers and support services providers to ensure that their equipment, facilities, or services comply with CALEA's assistance capability requirements. Congress, by including section 106, recognized that manufacturers and support service providers play a critical role in the conduct of lawful electronic surveillance, and without their assistance, carriers would be unable to comply.

Accordingly, manufacturers and support service providers are required to make available all features or modifications necessary to meet CALEA's assistance capability requirements. In return, manufacturers and support services providers are to be paid a reasonable fee by carriers in accordance with normally accepted business practices. Manufacturers or support service providers that fail to provide customers with necessary modifications may be subject to civil penalties under section 108 of CALEA.

#### **F. Section 107**

Section 107 of CALEA grants safe harbor to equipment manufacturers, telecommunications carriers, and support service providers that are in compliance with publicly available technical requirements or standards adopted by an industry association, standard-setting organization, or the FCC. Compliance with industry standards is voluntary; a carrier may, at its discretion, adopt other solutions for complying with the assistance capability requirements of section 103.

Section 107 also requires that the Attorney General consult with appropriate industry representatives and standards-setting organizations in developing CALEA requirements or technical standards. However, CALEA prohibits law enforcement from requiring that telecommunications carriers adopt a *specific* design or system configuration.

If industry associations or standard-setting organizations fail to adopt a technical standard, or if a government agency or any other person believes that industry-adopted standards are deficient as a means of meeting the assistance capability requirements of section 103, that party may petition the FCC to establish technical requirements or standards by rule. However, the FCC cannot make standards determinations or confer safe harbor if a deficiency petition has not been properly presented. Technical standards or requirements established by the FCC must:

- Meet the assistance capability requirements of section 103 by cost-effective methods;
- Protect the privacy and security of communications not authorized to be intercepted;
- Minimize the cost of such compliance on residential ratepayers;
- Serve the policy of the United States to encourage the provision of new technologies and services to the public; and
- Provide a reasonable time and conditions for compliance with the transition to any new standard, including defining the obligations of telecommunications carriers during the transition period.

##### **1. Development of an Industry Standard**

In early 1995, an ad hoc group, sponsored by the Telecommunications Industry Association (TIA) Subcommittee TR45.2, began working to develop an industry standard that would satisfy the assistance capability requirements of CALEA for wireline local exchange, cellular, and broadband PCS services. This effort included participation by industry and law enforcement.

A proposed industry standard was released for ballot in February, 1997. On December 5, 1997, TIA and Committee T1, sponsored by the Alliance for Telecommunications Industry Solutions (ATIS), announced the adoption and joint publication of an official interim industry technical standard, J-STD-025.

J-STD-025 defines the services and features necessary to support lawfully authorized

electronic surveillance and the interfaces used to deliver intercepted communications and call-identifying information to law enforcement. Although the interim technical standard was received favorably by industry, it was met with disfavor by both law enforcement and privacy organizations. Law enforcement argued that the interim standard was under-inclusive and failed to satisfy CALEA requirements because it did not include nine specific capabilities. The following table contains brief descriptions of these nine capabilities.

Name	Description
Content of subject-initiated conference calls	Capability that would enable law enforcement to access the content of conference calls supported by the subject's service.
Party Hold, Party Join, Party Drop	Messages would be sent to law enforcement that identify the active parties of a call. Specifically, on a multi-leg call, whether a party is on hold, has joined, or has been dropped from the call.
Access to subject-initiated dialing and signaling	Access to all dialing and signaling information available from the subject would inform law enforcement of a subject's use of features. (Examples include the use of flash-hook and other feature keys).
In-band and out-of-band signaling (Notification Message)	A message would be sent to law enforcement when a subject's <i>service</i> sends a tone or other network message to the subject or associate. This can include notification that a line is ringing or busy.
Timing to associate call data to content	Information necessary to correlate call identifying information with the call content of a communications interception.
Post-cut-through dialed digits (dialed digit extraction)	Extraction and delivery on a call data channel of call-routing digits dialed by a subject after the initial call setup is completed.

Surveillance Status Message	Message that would provide the verification that an interception is still functioning on the appropriate subject.
Continuity check (C-Tone)	Electronic signal that would alert law enforcement if the facility used for delivery of call content interception has failed or lost continuity.
Feature Status Message	Message that would provide affirmative notification of any change in a subject's subscribed-to features.

By contrast, privacy organizations, such as the Center for Democracy and Technology (CDT), Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), and American Civil Liberties Union (ACLU), argued that the interim technical standard was over-inclusive because it included access to information that identified the location of an intercept subject and failed to protect the privacy of packet-switched communications. CDT also argued that the additional capabilities sought by law enforcement were not required under CALEA and would further render the industry standard deficient.

By April 1998, the FCC had received four official petitions requesting that it establish, by rule, technical requirements and standards for CALEA compliance. The FCC responded, launching what would become a protracted debate, by issuing a public notice and soliciting comments on the petitions.

On August 31, 1999, the FCC issued a Third Report and Order, adopting technical requirements for wireline local exchange, cellular, and broadband PCS services. Communications Assistance for Law Enforcement Act 64 Fed. Reg. 51,710 (Sept. 24, 1999). In remanding the interim standard to the TR45.2 subcommittee for modification, the FCC ruled that telecommunications carriers will be required to implement all of the capabilities included in J-STD-025 (the interim technical standard), plus six of nine missing capabilities requested by law enforcement. The subcommittee was allowed seven months, or until March 30, 2000, to complete necessary changes to J-STD-025, in accordance with the FCC ruling. The six missing

---

capabilities determined by the FCC to be required by CALEA include: content of subject-initiated conference calls; party-hold, party-join, and party-drop messages; access to subject initiated dialing and signaling; in band and out-of-band signaling; timing; and post-cut-through dialed digits. The FCC further ruled that while CALEA did not require carriers to provide the remaining three missing capabilities, carriers may offer the capabilities to law enforcement at their discretion.

The FCC did not modify the technical requirements of J-STD-025 for packet-mode communications. Instead, it permits packet-mode data to be delivered to law enforcement in accordance with the interim technical standard, pending further study of packet-mode communications by the telecommunications industry.

On November 16, 1999, members of the telecommunications industry filed suit in the United States Court of Appeals challenging certain elements of the FCC's Third Report and Order. *United States Telecom Ass'n v. F.C.C.*, 227 F.3d 450 (D.C. Cir. 2000). On August 15, 2000, the United States Court of Appeals rendered a decision regarding the FCC's Third Report and Order. The Court vacated a portion of the FCC's order, and remanded the following capabilities to be reassessed by the FCC on the grounds that the FCC did not adequately substantiate its conclusions: (1) party-hold, party-join, and party-drop messages; (2) access to subject initiated dialing and signaling; (3) in-band and out-of-band signaling; and (4) post-cut-through dialed digits. The Court upheld the FCC's conclusions regarding location information and packet-mode communications.

## 2. Compliance Extensions

Section 107 also authorizes the FCC to extend the date for compliance with the assistance capability requirements of section 103. In a Memorandum Opinion and Order, released on September 11, 1998 (CC docket No.97-213, FCC 98-233), the FCC exercised this authority by extending the deadline for compliance from October 25, 1998, to June 30, 2000.

The FCC, in its Third Report and Order, established a separate compliance deadline for implementation of the six missing capabilities. Wireline local exchange, cellular, and broadband PCS carriers will be required to make the six punch list capabilities available to law enforcement by September 30, 2001.

## G. Section 108

Section 108 establishes conditions for the issuance of an enforcement order directing a carrier, a provider of support services, or a manufacturer of telecommunications equipment to comply with CALEA, including compliance requirements and limitations on the scope of an enforcement order.

### 1. Issuance of an Enforcement Order

Section 108(a) establishes conditions for which a court may issue an enforcement order under 18 U.S.C. § 2522. First, a court must find that alternative technologies, capabilities, or facilities are not reasonably available to law enforcement, and that compliance is or would have been reasonably achievable had timely action been taken by a carrier, a provider of support services, or a manufacturer. A court may impose a civil penalty of up to \$10,000 per day against a carrier, a provider of support services, or a manufacturer for each day in violation.

### 2. Compliance with an Enforcement Order

Under section 108(b), a court shall specify a reasonable time period for compliance considering the good faith efforts of the violating entity to comply, the effect upon the entity's ability to continue to conduct business, the entity's degree of culpability, and other matters as justice may require.

### 3. Limitations of an Enforcement Order Directing a Carrier

Section 108(c), imposes three limitations on the scope of an enforcement order. First, an enforcement order may not require a carrier to comply with a surveillance request that requires the use of capacity for which the Attorney General has not agreed to reimburse the carrier. Second, an enforcement order may not require a carrier to comply with a capability requirement that the

---

FCC has determined is not “reasonably achievable,” unless the Attorney General has agreed to reimburse the carrier for necessary modifications. Third, no enforcement order can require a carrier to modify its equipment, facilities, or services, installed before January 1, 1995, unless the Attorney General has agreed to pay all reasonable costs of the modification or there has been a significant upgrade.

#### **H. Section 109**

Section 109 establishes reimbursement guidelines for two categories of equipment, facilities, and services:

1. Equipment, Facilities, and Services Installed or Deployed on or Before January 1, 1995

Under section 109(a), the Attorney General is authorized to pay all reasonable costs directly associated with modifications to equipment, facilities, and services installed or deployed on or before January 1, 1995, to achieve the assistance capability requirements of section 103.

If the Attorney General elects not to reimburse a carrier for modifications, such equipment, facilities, and services are deemed to be in compliance with CALEA and are not subject to enforcement under section 108. If, however, the carrier subsequently replaces, significantly upgrades, or modifies the equipment, the grant of compliance will be rescinded, and the carrier required to comply with provisions governing equipment, facilities, and services installed or deployed after January 1, 1995.

2. Equipment, Facilities, and Services Installed or Deployed after January 1, 1995

The Attorney General is authorized to reimburse telecommunications carriers for modifications to equipment, facilities, and services installed or deployed after January 1, 1995, only if the FCC determines that compliance is not "reasonably achievable." Whether compliance is “reasonably achievable” depends on a number of factors spelled out in section 109(b), including whether compliance would “impose

significant difficulty or expense on the carrier or on . . . users of the carrier’s systems.”

If the FCC determines that compliance is not reasonably achievable, the Attorney General may either reimburse the carrier for all costs in excess of what the FCC finds to be reasonable or consider the carrier to be in compliance with the assistance capability requirements of section 103.

3. Cost Recovery Regulations

Section 109 also requires that the Attorney General, after notice and comment, establish regulations to facilitate carrier reimbursement as authorized under CALEA, including reimbursement under 18 U.S.C. § 2518(4), 18 U.S.C. § 3124, and 50 U.S.C. § 1802 (the Foreign Intelligence Surveillance Act). The Attorney General satisfied this obligation with the publication of the CALEA Cost Recovery Regulations on March 20, 1997. Implementation of Section 109 of the Communications Assistance for Law Enforcement Act, 62 Fed. Reg. 13,307 (March 20, 1997) (codified at 28 C.F.R. Part 100). The published rules establish standard recovery procedures for carriers seeking reimbursement under section 109.

4. Nationwide Right-to-Use Licenses

The FBI has implemented a reimbursement strategy that allows telecommunications carriers to receive CALEA software at no charge for certain high priority switching platforms. Under nationwide right-to-use license agreements, the FBI pays for the development of CALEA software solutions for high priority switching platforms. This allows telecommunications carriers to receive CALEA software at a nominal charge for equipment, facilities, or services installed or deployed now and in the future.

#### **I. Section 110**

When CALEA was enacted into law in 1994, Congress *authorized* \$500 million to be appropriated to reimburse the telecommunications industry for certain eligible costs associated with modifications to their networks. This dollar amount was authorized to remain available until expended. CALEA was subsequently amended by The Omnibus Consolidated Appropriations Act of

1997, which created the Telecommunications Carrier Compliance Fund (TCCF) and appropriated \$60 million in initial CALEA funding. The purpose of the TCCF is to facilitate the disbursement of funds available for CALEA implementation. Additionally, the Act authorized agencies with law enforcement and intelligence responsibilities to transfer unobligated balances into the TCCF, subject to applicable Congressional reprogramming requirements.

The following table illustrates the dollar amounts and timing of Congressional appropriations and fund transfers from authorized agencies with law enforcement and intelligence responsibilities.

TELECOMMUNICATIONS CARRIER COMPLIANCE FUND ACTIVITY	
Activity	Amount
FY 1997 Direct Appropriations	\$60,000,000
FY 1997 Department of Justice Working Capital Fund	\$40,000,000
FY 1997 United States Postal Inspection Service Transfer	\$1,000,000
FY 1997 United States Customs Service Transfer	\$1,580,270
FY 2000 Direct Appropriations	\$15,000,000
FY 2000 Supplemental Appropriations	\$181,000,000
FY 2001 Direct Appropriations	\$200,977,000
<b>TOTAL DEPOSITS</b>	<b>\$499,557,270</b>

#### J. Section 111

Section 111 establishes the effective date for compliance with provisions of Section 103 and 105. These deadlines have since been revised by the FCC to accommodate industry promulgation of a technical standard and the development of technical solutions.

#### K. Section 112

Section 112 ensures that both congressional and public oversight of CALEA is maintained by requiring the submission of reports by the Attorney General. This section also specifies reporting requirements for the Comptroller General that includes describing the type of equipment, facilities, and services that have been brought into compliance and reflecting the cost effectiveness of the payments made by the Attorney General.

#### IV. Further Information

As stated previously, the CALEA Implementation Section (CIS) of the FBI has been delegated implementation responsibilities and represents the interests of the law enforcement community in matters pertaining to CALEA. CIS has established a website, [www.askcalea.net](http://www.askcalea.net), in order to disseminate implementation details and provide an avenue for requesting additional information.

#### ABOUT THE AUTHOR

CALEA Implementation Section (CIS) was established in 1995 in response to the delegation of implementation responsibilities to the Federal Bureau of Investigation (FBI) by the Attorney General. CIS spearheads CALEA implementation efforts by fulfilling the responsibilities assigned to the Attorney General through consultation with the telecommunications industry and privacy advocates. CIS represents the interests of the entire law enforcement community before Congress, other government agencies involved in the implementation of CALEA, and the telecommunications industry. CIS is headed by Section Chief, Supervisory Special Agent Michael P. Clifford, a 21 year veteran of the FBI. CIS maintains a website, [www.askCALEA.net](http://www.askCALEA.net), where more information is available and specific questions can be submitted regarding CALEA implementation activities.

---

---

# Novel Criminal Copyright Infringement Issues Related to the Internet

*David Goldstone*  
Trial Attorney  
Computer Crime and Intellectual Property  
Section  
Team Leader, Intellectual Property Team

*Michael O'Leary*  
Trial Attorney  
Computer Crime and Intellectual Property  
Section

Copyright law is based on a simple premise enshrined in Anglo-American legal tradition: For a limited time, an original work in fixed form may not be copied (or otherwise infringed) without the permission of the copyright holder. The basis of copyright in federal law is as old as the Constitution, U.S. Const. art. I, § 8, cl. 8; infringement of a copyright has been a federal crime since 1909. *See* Act of March 4, 1909, ch. 28, 35 Stat. 1082. The legal right of control over a creative work has long been recognized as an essential incentive for authors to create such works.

Congress has distilled the crime of felony copyright infringement to four essential elements: (1) a copyright exists; (2) it was infringed by the defendant, specifically by reproduction or distribution of the copyrighted work; (3) the defendant acted “willfully”; and (4) the defendant infringed at least 10 copies of one or more copyrighted works with a total retail value of more than \$2,500 within a 180-day period. *See* 17 U.S.C. § 506(a)(2); 18 U.S.C. § 2319(a), (c)(1). Further elaboration on these elements, if necessary, can be found in the recently published manual, *Prosecuting Intellectual Property Crimes* (2001) (<http://www.cybercrime.gov/ipmanual.htm>). Criminal copyright infringement is discussed in depth in chapter III of the manual.

The recent development of computer technology — most notably the Internet — has had a complex and profound effect on the dissemination of copyrighted works, by the copyright holder and by infringers alike. Both the supply of, and the demand for, copyrighted works have escalated dramatically because of the Internet’s success as a communications medium, the large number of people worldwide who use it, and the ease with which materials may be made available for copying. Media products produced today, including software and music, are often in a digital format, which permits fast, cheap, and easy production of copies (legitimate or infringing) identical in quality to the original. The digital nature of today’s media products also makes them much easier to distribute in large scale over the Internet. Some so-called “warez” Web sites are dedicated, either entirely or in part, to providing widespread access to copyrighted materials. In addition, people have developed new technologies that facilitate copying via the Internet. One fact is clear: the Internet, computers, and related developments in technology have altered, and will continue to profoundly alter, the ease with which people may reproduce and distribute copyrighted works.

In Internet-based copyright cases, experience has shown that certain issues arise regularly: (1) large scale infringement without profit motive; (2) disclaimers; (3) unusual proof issues for quantity, loss, and identity; and (4) sympathetic defendants including juveniles. Moreover, Internet-based copyright cases often involve complex, emerging technologies, which raise unique legal and technical issues that require additional background, including: (1) novel means of infringement; (2) facilitation; (3) audio compression technology such as MP3; and (4) file sharing technologies. Each of these subjects is discussed below.

---

In addition, defendants in Internet copyright cases are especially prone to raise First Amendment claims in preliminary discussions. No such claim has ever been discussed in a published criminal case, perhaps because criminal copyright infringement requires proof of the defendant's willfulness. Nevertheless, it has long been recognized that civil enforcement of copyright laws in America can sometimes be at tension with the constraints of the First Amendment. *See, e.g.*, Paul Goldstein, *Copyright and the First Amendment*, 70 Colum. L. Rev. 983 (1970); Melville B. Nimmer, *Does Copyright Abridge the First Amendment Guarantees of Free Speech and Press?*, 17 UCLA L. Rev. 1180 (1970). New technologies such as the Internet provide fertile ground for revisiting these conflicts. *See, e.g.*, John Gladstone Mills III, *Entertainment on the Internet: First Amendment and Copyright Issues*, 79 J. Pat. & Trademark Off. Soc'y 461 (1997). Prosecutors should be aware of the potential First Amendment limitations when charging cases under novel theories of copyright law.

## **I. Common Issues in Internet Copyright Cases**

### **A. Large Scale Infringement Without Profit Motive**

Infringement without profit motive is far more common in cases of Internet-based copyright infringement than it is in the physical world. Until recently, the prosecution was required to prove that copyright infringement was done willfully and for commercial advantage or private financial gain. Now the law provides for prosecution in the absence of these monetary considerations. Specifically, the current statute, as codified at 17 U.S.C. § 506(a)(2), allows for prosecution in cases involving large scale illegal reproduction or distribution of copyrighted works where the infringers act willfully, but without a discernible profit motive. Congress specifically made this change as part of the No Electronic Theft (NET) Act of 1997, Pub. L. No. 105-147, 111 Stat. 2678. This statutory amendment was enacted as a response to *United States v. LaMacchia*, 871 F. Supp. 535 (D. Mass. 1994), in which a Massachusetts District Court held that electronic piracy of copyrighted works, which could not be prosecuted under then-existing copyright

infringement laws if the defendant did not realize a commercial advantage or financial gain, could not be charged as a wire fraud. For a more extended discussion of charging mail or wire fraud in infringement cases, see *Prosecuting Intellectual Property Crimes* § VI.B.1 (<http://www.cybercrime.gov/ipmanual/06ipma.htm#VI.B.1>).

Cases alleging illegal distribution of copyrighted materials without commercial gain have been charged all over the country. In August 1999, the first person was convicted for illegally posting computer software programs, musical recordings, and digitally-recorded movies on his Web site, and allowing the general public to download and copy these products free of charge. The Oregon defendant pleaded guilty to a felony. *See* United States Attorney's Office, District of Oregon, *First Criminal Copyright Conviction Under the "No Electronic Theft" (NET) Act for Unlawful Distribution of Software on the Internet*, August 20, 1999 (<http://www.cybercrime.gov/netconv.htm>). In addition to Oregon, other significant cases have been charged in the Northern District of California, the District of Columbia, the Northern District of Illinois, and the Eastern District of Michigan without allegation of commercial gain. For additional information about cases charged under the NET Act, see <http://www.cybercrime.gov/iplaws.htm#Xb>.

Prosecutors should not hesitate to utilize this avenue of enforcement. In many cases the damage to the victim may be enormous although the infringer is not profiting financially. In fact, because the copyrighted materials are provided without charge to the entire Internet-using public, the demand for the infringing goods provided for free may increase dramatically and result in great potential loss to the rights holder.

### **B. Disclaimers**

Internet sites offering copies of infringing materials frequently provide so-called "disclaimers" in an attempt to immunize their operators from criminal liability by establishing a good faith defense. Although such disclaimers could conceivably be evidence of the operator's good faith, in many cases they can actually be

---

helpful evidence of the defendant's awareness of the law, and thus be used to establish willfulness. For example, in *United States v. Gardner*, 860 F.2d 1391, 1396 (7th Cir. 1988), the Seventh Circuit rejected the defendant's assertions that his disclaimer shifted responsibility to the purchaser and concluded that "such statements establish that he was well aware that his actions were unlawful." See *United States v. Knox*, 32 F.3d 733, 753 (3d Cir. 1994) (rejecting defendant's argument that disclaimers in brochure stating that child pornography videos were legal disproves the *mens rea* element and concluding that "[i]f anything, the need to profess legality should have alerted Knox to the films' dubious legality"); see also *Rice v. Palladin Enters., Inc.*, 128 F.3d 233, 254 (4th Cir. 1997) (observing that a jury could readily find the "For academic study only!" disclaimer in promotional sales catalogue for *Hit Man* book "to be transparent sarcasm designed to intrigue and entice"); *ON/TV of Chicago v. Julien*, 763 F.2d 839, 844 (7th Cir. 1985) ("Whatever the attempted legal effect of the defendant's disclaimer, the ultimate trier of fact could easily find that it was a transparent attempt to deny the patent illegality of the defendant's acts. . . ."); *Time Warner Entertainment/Advance-Newhouse Partnership v. Worldwide Elecs., L.C.*, 50 F. Supp. 2d 1288, 1296-97 (S.D. Fla. 1999) ("[C]ourts have found that a pirate decoder seller's use of such disclaimers reflects their awareness of the illegality of their business." (citing cases)); cf. *Direct Sales v. United States*, 319 U.S. 703, 712-13 (1943) (holding that jury may infer intent to assist a criminal operation based upon a drug distributor's marketing strategy). For a discussion of proving willfulness in copyright cases, see *Prosecuting Intellectual Property Crimes* § III.B.3 (<http://www.cybercrime.gov/ipmanual/03ipma.htm#III.B.3>).

### **C. Proof Issues: Quantity, Loss, and Identity**

A few proof issues commonly arise in Internet copyright cases. One challenge for Internet cases can be to accurately determine the identity and quantity of the infringing items (pirated copyrighted works) that were distributed. While it may be relatively easy to determine the identity of

the pirated works made available on a site, it can be a challenge to determine the identity and quantity of the works actually downloaded or distributed. For example, in order to initiate a felony copyright prosecution under 18 U.S.C. § 2319, the government must establish that at least ten illegal copies were made during a 180-day period, with a total value exceeding \$2,500. In developing the required proof, it can be quite helpful if the entity hosting the Web site keeps specific logs.

Establishing the quantity of specific copied works is important to accurately establish a loss figure for sentencing as well. The Sentencing Guidelines were recently amended to take into account some of these difficulties. For example, effective May 1, 2000, a sentencing enhancement is applicable if the defendant uploads a copyrighted work to an Internet site with the intent to allow others to download or otherwise access the infringing item. Moreover, under the new guideline, where the infringing item is a digital or electronic reproduction of the infringing item (as is typical in Internet copyright cases), the "infringement amount" is based on the retail value of the *infringed* (i.e., legitimate) item, multiplied by the number of infringing items. See U.S. Sentencing Commission, *Guidelines Manual* § 2B5.3 (Nov. 1998 & Supp. 2000); See also *Prosecuting Intellectual Property Crimes* § VII.A (2001) (<http://www.cybercrime.gov/ipmanual/07ipma.htm#VII.A>). Even under this new guideline, presenting evidence of the number of infringing items is an important part of the government's case.

While each investigation may employ different techniques, law enforcement agencies should utilize all available resources in identifying victims and determining loss. In certain circumstances, assistance might be sought from the private sector. Certain private industry business associations, such as the Business Software Alliance, the Interactive Digital Software Association, the Motion Picture Association of America, the Recording Industry Association of America, and the Software Information Industry Association, have provided significant assistance in previous investigations.

---

For a listing of industry contacts, see *Prosecuting Intellectual Property Crimes* App. A (<http://www.cybercrime.gov/ipmanual/appa.htm>)

Assuming an investigation establishes that a particular Web site is a significant source of copyright infringement, effective prosecution will also require that the government link the defendant to that Web site. Although each Web site will have a domain name, and arguably a corresponding domain name registration, it is possible and perhaps probable that much of that information will be falsified in order to shield the criminal's identity. Care must be taken to meet the burden of showing that the defendant is in fact responsible for the infringement taking place. With regard to an Internet infringement case, this will likely require a showing that the defendant maintained some form of knowing control over the content and maintenance of the subject Web site.

#### **D. Sympathetic Defendants, Including Juveniles**

In online infringement cases, the defendant may be young, have no criminal record, or otherwise be sympathetic to a jury. In such cases, the government should be able to provide a basis for a determination that the defendant was, in fact, acting egregiously and was not merely engaged in technical violations of the law. While the means of overcoming this hurdle will vary from case-to-case, some factors to show that the defendant was acting egregiously include establishing: (1) a significant amount of infringement; (2) the infringing activity occurred repeatedly over a lengthy period of time; (3) the defendant was so involved in the infringement as to lead, unavoidably, to the conclusion that his or her actions were willful; (4) the defendant in some way profited from the conduct; (5) communications reflecting malice or other criminal intent; and (6) if applicable, some of the copyrighted works belonged to smaller companies, whose profitability may be jeopardized by the defendant's conduct.

If the defendant is a juvenile, options for federal prosecutors are limited. The Federal Government may proceed against juveniles in federal court for acts of juvenile delinquency

other than a crime of violence or a crime involving a controlled substance only if the Attorney General, or his or her designee for these purposes, certifies that the applicable juvenile or state court has declined prosecution of the juvenile, or the state does not have available programs and services adequate for the needs of juveniles. See 18 U.S.C. § 5032. Prosecutors confronted with juvenile defendants are encouraged to review the *United States Attorneys' Manual* § 9-8.00. They should also consult any experts on juvenile prosecutions in their office. Transferring a person from juvenile status to adult status requires consultation with the Terrorism and Violent Crime Section of the Criminal Division, which can be reached by calling (202) 514-0849. Prosecutors may want to consult with attorneys from that section even if they do not seek a transfer. In appropriate circumstances, prosecutors should fully consider the option of federal prosecution. Otherwise, prosecutors should consider referring a case involving a juvenile to state authorities. See *Prosecuting Intellectual Property Crimes* Section VI.A.2 (<http://www.cybercrime.gov/ipmanual/06ipma.htm#VI.A.2>.) for additional discussion of state prosecution issues. A listing of state IP laws is provided at Appendix F. See *Prosecuting Intellectual Property Crimes* Section App. F (<http://www.cybercrime.gov/ipmanual/appf.htm>)

#### **II. Challenges of Emerging Technology**

Increasingly advanced software enables criminals to violate intellectual property rights more quickly, more frequently, and with better quality than in the past. Prosecutors may consider investigating some of the individuals who develop, utilize, and distribute these technologies. In so doing, it is essential that prosecutors understand the underlying technologies in order to appropriately differentiate lawful from unlawful conduct and to address potentially novel challenges that these technologies may present. Because the legal treatment of certain advanced reproduction technologies may be unsettled, consultation with the Computer Crime and Intellectual Property Section is strongly encouraged when evaluating these cases.

---

## A. Novel Means of Infringement Generally

The Internet facilitates infringement, particularly reproduction and distribution, in a variety of novel ways. Unauthorized copies of works may be published or posted on Web sites, or made available through other technological means. For example, they may be uploaded (“posted”) to the Usenet, a group of separate bulletin boards allowing users to carry on discussions by posting questions, comments, files, and information on various topics. It is possible to copy the work to numerous Usenet bulletin boards at once (“cross-posting”). Other technological means of distributing works are sites designed merely to transfer files by means of the file transfer protocol (“FTP sites”) or chat rooms for those interested in copying files, most commonly occurring on chat rooms run under the Internet Relay Chat (“IRC”) protocol.

Making unauthorized copies of works available to the public for reproduction and distribution can be infringement even if it is done through a cutting edge medium such as an Internet Web site. *See, e.g., Michaels v. Internet Entertainment Group, Inc.*, 5 F. Supp.2d 823, 834 (C.D. Cal. 1998) (publishing copyrighted videotape on Internet Web site constitutes infringement of plaintiff’s right to distribute work). To show distribution, it is not necessary to prove that others actually copied or used the work, only that the defendant knowingly made it available to the public. *See Hotaling v. Church of Jesus Christ of Latter-Day Saints*, 118 F.3d 199, 203 (4th Cir. 1997) (distribution occurs when all steps necessary to make a work available to the public have been completed, regardless of whether persons actually used the work).

In criminal cases, of course, copyright liability against service providers for transmitting infringing materials is limited by the government’s burden of proving that the infringement was done “willfully.” *See Prosecuting Intellectual Property Crimes* § III.B.3 (<http://www.cybercrime.gov/ipmanual/03ipma.htm#III.B.3>) (discussing “wilfulness” requirement under criminal copyright infringement). Even in civil cases, courts have examined whether a bulletin board service or Internet Service Provider

(ISP) can be liable for infringement—whether under theories of direct or contributory infringement or, alternatively, vicarious liability—if it merely provides the means to store or transmit files that other parties upload and subsequently download. *See, e.g., Playboy Enters., Inc. v. Chuckleberry Publishing, Inc.*, 939 F. Supp. 1032, 1040, 1044-45 (S.D.N.Y. 1996) (requiring bulletin board system based in Italy that contained infringing images to shut down or to refrain from accepting subscriptions from customers living in the United States); *Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995) (granting defendant’s motion for summary judgment as to direct and vicarious copyright infringement, but not as to contributory copyright infringement for provision of access to Usenet newsgroup system and Internet access server that facilitated dissemination of infringing works over the Internet where the plaintiff’s raised a genuine issue of fact regarding whether the defendant had adequate knowledge after receiving a notice letter from plaintiffs). In these and similar cases, courts have attempted to differentiate between passive and active providers. Passive providers generally facilitate transfers without human intervention and without looking at the content of files which users transfer. Active providers have taken some affirmative action, such as attempting to control content of user uploads, and are therefore considered more responsible for infringement than passive providers.

Any assessment of service provider liability should also be considered in light of Congress’ reaction to the issue—the enactment of the Online Copyright Infringement Liability Limitation Act, Pub. L. No. 105-304, 112 Stat. 2877 (1998), which significantly circumscribes the conditions under which online service providers might incur liability. *See* 17 U.S.C. § 512. This section provides limitation for infringement in four different scenarios:

- Transmissions. Automatically transmitted communications (such as electronic mail messages) that are not modified or edited by the service provider and that are not maintained any longer than reasonably necessary, 17 U.S.C. § 512(a);

- 
- Caching. System caching of materials requested by users (such as popular Web pages) on behalf of subsequent users as long as the service provider complies with industry standard data protocols, 17 U.S.C. § 512(b);
  - Storage. Information residing on systems at the direction of users (such as a hosted Web site) as long as the service provider does not have knowledge of the infringement or financial benefit directly attributable to the infringing activity and where the service provider, upon notification, removes the infringing materials, 17 U.S.C. § 512(c); and
  - Linking. Information location tools (such as a hypertext link) referring or linking users to an online location containing infringing material or infringing activity as long as the service provider does not have knowledge of the infringement or financial benefit directly attributable to the infringing activity and where the service provider, upon notification, removes the infringing materials or the access to them, 17 U.S.C. § 512(d).

Section 512 also provides a process by which copyright holders may notify service providers of allegedly infringing activities and service providers have certain duties to respond and by which injunctive or other relief may be sought. See 17 U.S.C. § 512(g)-(j). See also *A&M Records, Inc. v. Napster, Inc.*, No. C99-05183 MHP, 2000 WL 573136, at \*10 (N.D. Cal. May 12, 2000) (holding that Internet-based file sharing service does not meet requirements of “safe harbor” under 17 U.S.C. § 512(a)).

It is common that certain forms of intellectual property, such as computer software, are sold pursuant to a license that governs the use, including reproduction and distribution, of the intellectual property itself. Copyright law expressly provides that the exclusive rights of ownership may be transferred in whole or in part by conveyance. 17 U.S.C. § 201(d). Where a valid license is provided, activities such as reproduction and distribution within the scope of that license are not infringing.

## **B. Facilitation**

One aspect of potential copyright infringement on the Internet is acting as a facilitator for copying. Because of the apparently seamless nature of the Internet, a facilitator of infringement who actively encourages it can cause much more infringement than the party that provides the unprotected work for copying. Facilitation can be exemplified by “linking,” or “deep linking.” A link is a reference on one web page to a different web page. Often, the link takes the viewer directly to the other web page when the viewer clicks on the link. In terms of copyright infringement, the primary concern for prosecutors will be links to sites conducting illegal activity, particularly sites that allow copying of copyrighted materials (“warez sites”).

One question for prosecutors will be how to address an individual who, while not illegally offering the software on his or her site, establishes a direct link to a “warez site” that is offering illegal software. While a target who illegally offers copyrighted software on a “warez site” is engaging in infringement, criminality is less clear if the copyrighted software is on another site to which the target simply links.

In these instances, the facts surrounding the activity will be critical. For example, is the target’s “warez site” effectively encouraging the infringement? Is there independent evidence, in addition to or aside from the “warez site,” which suggests intent to infringe? Is there evidence of some illicit relationship between the target or the target’s “warez site” and the site containing the copyrighted work to be downloaded? Further, what if the target links not to the beginning of the secondary site, but further or deeper into the site, directly to the downloadable software? This is known as “deep linking,” when the link bypasses initial portions of a Web site and takes the user to a specific place within the targeted Web site. Prosecutors should consider the relative culpability of an individual who links a user directly to a copyrighted work and one who links the user to a site that offers the illegal software, possibly in addition to other legal information or services.

---

These questions illustrate the prosecutorial challenges posed by infringers' skillful use of links. The activity may be more analogous to the theories of contributory, or, if the requisite level of control exists, vicarious infringement (developed civilly), than direct infringement. Accordingly, given the appropriate facts and circumstances, prosecutors may wish to pursue prosecution, if at all, under an aiding and abetting theory rather than as simple infringement.

Online service providers may have potential civil liability as facilitators as well. Courts have found that service providers have infringed by reproduction if the provider knowingly copied protected works without authorization. *See, e.g., Playboy Enters., Inc. v. Webbworld, Inc.*, 991 F. Supp. 543 (N.D. Tex. 1997) (defendant infringed by copying images from other Internet locations, creating smaller "thumbnail" versions of the images, and charging a fee to view these thumbnail images via the defendant's Web site), *aff'd*, 168 F.3d 486 (5th Cir. 1999); *Religious Tech. Ctr v. Netcom On-Line Communication Servs., Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995) (finding possible liability depending on defendant's knowledge, for contributory copyright infringement for provision of access to Usenet newsgroup system and Internet access server that facilitated dissemination of infringing works over the Internet).

In order to address online service provider liability and to remove it under certain circumstances, the Online Copyright Infringement Liability Limitation Act was signed into law in 1998. As outlined above, it limits, in a number of online contexts, liability of service providers. Pub. L. No. 105-304, 112 Stat. 2877 (codified at 17 U.S.C. § 512). Prosecutors should be cognizant of this provision when the conduct of an online service provider is at issue. For facilitation issues, prosecutors should give special attention to 17 U.S.C. § 512(d) which limits the circumstances under which a service provider may be liable for infringement because it utilizes technologies or tools to link users to copyrighted works.

### **C. Audio Compression Technology Such as MP3**

One well-known technology which has enhanced the public's ability to copy music is a compression technology known as "MP3." Short for MPEG-1 Audio Layer 3, MP3 uses a format originally designed for video to compress audio files at a ratio of 12:1. The MP3 technology takes audio signals from the original recording and compresses them into a smaller, more easily transferable format without sacrificing the quality of the sound. Because MP3 preserves the high quality of the sound recording, and is increasingly popular among the public, portable MP3 players are being marketed for personal use. While many people utilize MP3 technology lawfully, individuals can also use this technology to sell or distribute a high volume of illegally obtained sound recordings with relative ease. *See, e.g., Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc.*, 180 F.3d 1072, 1073 (9th Cir. 1999) (describing advent of MP3 digital technology and holding that hand-held audio device that receives, stores, and plays MP3 audio files, but does not record them directly from digital music recordings, does not violate prohibitions of the Audio Home Recording Act). Moreover, applications have developed utilizing technologies such as MP3 to provide greater access to audio files on the Internet. One online service, which made MP3 files of copyrighted audio recordings available via the Internet, was sued for copyright infringement. In ongoing litigation, the court has found that the defendant's conduct violated the copyright laws, that it had done so "willfully," and that its activities did not constitute "fair use." *See, e.g., UMG Recordings, Inc. v. MP3.COM, Inc.*, No. 00 CIV. 472 (JSR), 56 U.S.P.Q.2d 1376 (S.D.N.Y. Sept. 6, 2000); *UMG Recordings, Inc. v. MP3.COM, Inc.*, 92 F. Supp. 2d 349, 351-52 (S.D.N.Y. 2000).

### **D. File Sharing Technologies**

Increasingly, software-based technologies have been developed to facilitate the sharing of files with ease. For example, Napster (<http://www.napster.com>) is a well-known online service which allows individuals to access and share files, such as MP3 files, belonging to other

---

people via the Internet. Essentially, Napster creates a community of users with files—the size of the community depends upon who is signed on at a given time. The files are not located on the Napster server, but rather on the computers of the individual users. Napster provides software to link these users together. Amid allegations of contributory and vicarious copyright infringement, Napster has been sued civilly by the recording industry. *See A&M Records, Inc. v. Napster, Inc.*, No. C99-05183 MHP, 2001 WL 227083 (N.D. Cal. March 5, 2001) (issuing order enjoining Napster “from engaging in, or facilitating others in, copying, downloading, uploading, transmitting, or distributing copyrighted sound recordings in accordance with this Order”), *on remand from, A&M Records, Inc. v. Napster, Inc.* 239 F.3d 2004 (9th Cir. 2001).

Other technological means can provide for file sharing as well. While Napster allows user searches for MP3 files to go through a central server, another application, Gnutella, directly links individual computers utilizing the software. This direct linking software allows one to reach hundreds of Gnutella users very quickly. *See, e.g., Lee Gomes, Gnutella, New Music-Sharing Software, Rattles the CD Industry*, Wall St. J., May 4, 2000, at B10 (reporting that on one evening there were over 1.5 million MP3 music recordings, computer programs, and other multimedia offerings available for free via Gnutella software). Gnutella and other analogous programs continue to evolve and improve as programmers develop the software and are generally available for free via the Internet.

Critics argue that these types of services and software compromise intellectual property rights and result in widespread infringement, be it directly or as a contributor. Supporters argue that the services may be used constructively to share many kinds of materials that are not copyrighted or are shared with the consent of the copyright holder. Moreover, supporters argue that creators of file-sharing programs such as Napster and Gnutella do not control or have no control over how the public utilizes them. While critics challenge the sufficiency of efforts to minimize liability, prosecutors must be aware of the often

difficult questions raised by these types of programs.

### III. Conclusion: Keeping Pace with Changing Technology

The examples highlighted here represent but a few of the many new software applications and services that greatly improve the public’s ability to locate and copy protected materials online. There seems little question that over time, these technologies will not only improve, but will be surpassed by more efficient, faster, perhaps more discreet applications that further enhance the ability to copy online. Some of these applications may be designed to operate at the margin of what is proper under the copyright law, or just beyond it. A key question in these developing criminal cases under these circumstances is evidence of willfulness. As these examples illustrate, however, prosecutors will need to think critically about emerging technologies, and how they operate and are used, in order to keep pace with online infringers.

#### ABOUT THE AUTHORS

**David Goldstone** has been a trial attorney in the Computer Crime and Intellectual Property Section for four years. He is the Team Leader for the Intellectual Property Team, and the principal author of *Prosecuting Intellectual Property Crimes* (2001). Mr. Goldstone has been an instructor at the National Advocacy Center and is an adjunct professor of cyberspace law at the law schools of Georgetown University and George Washington University.

**Michael O’Leary** is a trial attorney in the Computer Crime and Intellectual Property Section. O’Leary initially joined the Department of Justice in the Office of Legislative Affairs in 1998. Prior to moving to the Justice Department he served as counsel to the United States Senate Committee on the Judiciary, including serving as counsel to the Subcommittee on Patents, Copyrights and Trademarks and as Chief Counsel to the Subcommittee on the Constitution. **a**

---

---

# The Economic Espionage Act of 1996: an Overview

George “Toby” Dilworth  
Assistant United States Attorney  
Computer and Telecommunications Coordinator  
District of Maine

In January 1998, Caryn Camp was unhappy with her job at IDEXX Laboratories, a world-leading manufacturer of veterinary diagnostics products based in Maine. She started searching the internet for another job, and sent an email with her resume to a company called Wyoming DNAVaccine (“WDV”). Steven Martin, WDV’s chief scientific officer, responded enthusiastically. Martin and Camp began corresponding regularly by email. Much of the early correspondence related to mundane topics about their lives in Maine and the west coast. However, as the correspondence progressed, Martin began emailing questions about IDEXX’s manufacturing methods, customer base, and pricing schedule. Camp emailed her answers back to Martin. After Camp expressed reservations about sending information to Martin and WDV, a potential competitor to IDEXX, Martin emailed her claiming that he did “not want to know anything confidential about IDEXX.” He said he only wanted public information.

After a brief hiatus, Martin resumed his questions regarding IDEXX’s procedures. He inquired about IDEXX’s fluorescent-based tests, as well as its customer base. If Camp did not know the answers to Martin’s questions, she researched them. She emailed him information about ongoing negotiations between IDEXX and a possible acquisition target, and shipped him copies of customer lists, manufacturing documents, and laboratory reports. On July 24, she mailed him the last shipment – a box filled with operating manuals, research and development data, and information about other competitors in the industry. She spent that evening doing her laundry and packing for an extended vacation to California, where she planned to

attend a family reunion and meet Martin for the first time. She wrote Martin a message describing the materials she had sent him, predicting that he would “feel like a kid on Christmas day” when he saw the contents. However, because she was tired and it was late at night, she made a terrible mistake. As she prepared to send the message, she went to the address book on her computer and inadvertently clicked on the address for John Lawrence, IDEXX’s global marketing director. Lawrence’s name was directly above Martin’s name in her address book. Camp immediately realized her error, and tried in vain to delete the message. She left for California the following morning, hoping that Lawrence would not read the message. Lawrence found Camp’s email meant for Martin and IDEXX notified the U.S. Attorney’s Office. In short order, the FBI executed search warrants at Camp’s home in Maine, and then Martin’s home and office in California.

So began *United States v. Camp and Martin*, CR 98-48-P-H (D.Me., Indictment filed Sept. 16 1988), one of the first cases brought under the Economic Espionage Act. Although the defendants were not well-funded and did not employ sophisticated espionage techniques, and IDEXX had taken substantial steps to protect its trade secrets, the defendants managed to make off with important proprietary information. They probably would have avoided detection except for Camp clicking on the wrong address in the early morning of July 25. Like other biotech companies, IDEXX had spent considerable resources developing these trade secrets. That a competitor could obtain them without incurring any costs posed substantial risks to IDEXX.

Over the past 40 years, extraordinary technological advances have improved lives and created economic growth. High speed communications systems, novel medical devices, and robotics are just a few examples. Most of these technological advances are based on trade

---

secrets – proprietary information which the owner keeps confidential.

Ironically, high tech advances have made it more difficult to protect those trade secrets. Vast amounts of information can be stored and transferred electronically without serious risk of detection. No longer does a disgruntled employee have to carry boxes of confidential files past the guard at the front door, nor does a competitor have to bribe an insider to deliver proprietary information. An unhappy employee or opportunistic licensee can abscond with a company's most important trade secrets simply by downloading them onto a floppy disk and walking out the front door with the disk in his pocket, or he can remain in his office and e-mail the information to a ready buyer. A competitor can steal trade secrets by gaining unauthorized access to the company's computers without ever leaving his home or office.

By 1996, Congress recognized the serious economic risks created by the theft of trade secrets from American companies. A 1995 survey of 325 companies determined that nearly half of them had experienced a trade secret theft. S. Rep. No. 104-359 (1996). It was estimated that nearly \$24 billion of corporate intellectual property was stolen every year. *United States v. Hsu*, 155 F.3d 189, 194 (3d Cir. 1998). The FBI suspected that more than twenty countries were actively trying to steal United States companies' trade secrets. Some warned that the end of the Cold War "sent government spies scurrying to the private sector to perform illicit work for businesses and corporations." *Id.* As the nation's workforce became more mobile, employees used their former employers' trade secrets for the benefit of their new employers, who had spent nothing to develop the information. Federal prosecutors often had difficulty fitting trade secret cases within the existing federal statutes. The National Stolen Property Act, 18 U.S.C. § 2314, did not apply to the theft of purely intellectual property. *See Dowling v. United States*, 473 U.S. 207, 216 (1985); *United States v. Brown*, 925 F.2d 1301, 1307-08 (10th Cir. 1991). Mail and wire fraud statutes did not always apply. The only federal statute explicitly targeting the theft of trade secrets was limited to government employees'

unauthorized disclosure of trade secrets, and offenders were subject only to misdemeanor penalties. 18 U.S.C. § 1905. States lacked the resources to investigate these crimes, and faced substantial jurisdictional hurdles. While more than 40 states had enacted some form of the civil Uniform Trade Secrets Act (UTSA), there was no effective criminal response to the problem.

Recognizing that intellectual property will play an increasingly important role in the national economy, and the ease with which it can be stolen and converted, Congress enacted the Economic Espionage Act of 1996 (the EEA), Pub. L. No. 104-294, 110 Stat. 3488. Congress intended the EEA to prohibit every type of trade secret theft, "from the foreign government that uses its classic espionage apparatus to spy on a company, to the two American companies that are attempting to uncover each other's bid proposals, or to the disgruntled former employee who walks out of his former company with a computer diskette full of engineering schematics." H.R. Rep. No. 104-788 (1996).

The EEA does not restrict competition or lawful innovation. According to the First Circuit, the EEA "was not designed to punish competition, even when such competition relies on the know-how of former employees of a direct competitor. It *was*, however, designed to prevent those employees (and their future employers) from taking advantage of confidential information gained, discovered, copied, or taken while employed elsewhere." *United States v. Martin*, 228 F.3d 1, 11 (1st Cir. 2000) (emphasis in original). Under the EEA, federal prosecutors have the means to help protect proprietary economic information. When he signed the bill, President Clinton predicted that the EEA "will protect the trade secrets of all businesses operating in the United States, foreign and domestic alike, from economic espionage and trade secrets theft and deter and punish those who would intrude into, damage or steal from computer networks." President William J. Clinton, Presidential Statement on the Signing of the Economic

---

Espionage Act of 1996 (Oct. 11, 1996) *available at* 1996 WL 584924.

## I. Two Distinct Parts

The EEA contains two distinct provisions. One addresses economic espionage directed by foreign governments or government-controlled entities. 18 U.S.C. § 1831. The other prohibits the commercial theft of trade secrets carried out for economic or commercial advantage, whether the perpetrator is foreign or domestic. 18 U.S.C. § 1832. While Congress apparently believed that foreign agents posed the greatest risk to American businesses and imposed more severe penalties against them, all of the prosecutions brought to date under the EEA have utilized section 1832. Because federal prosecutors have charged section 1832 more frequently, this article will address it first.

### A. Section 1832: Theft of Trade Secrets for Economic or Commercial Advantage

Under section 1832, the Government must prove beyond a reasonable doubt that: (1) the defendant stole, or without the owner's authorization obtained, sent, destroyed, or conveyed information; (2) the defendant knew or believed that the information was a trade secret; (3) the information was in fact a trade secret; (4) the defendant intended to convert the trade secret to the economic benefit of somebody other than the owner; (5) the defendant knew or intended that the owner of the trade secret would be injured; and (6) the trade secret was related to, or was included in, a product that was produced or placed in interstate or foreign commerce. It is also illegal to attempt to steal a trade secret, or to receive, purchase, destroy, or possess a trade secret which the defendant knew was stolen. 18 U.S.C. §§1832(a)(2) - (4).

Unlike most other types of property, a trade secret may be stolen without ever leaving the custody or control of its owner. Congress recognized this fact, and prohibited copying, duplicating, sketching, drawing, photographing, downloading, uploading, altering, destroying, photocopying, replicating, transmitting, delivering, sending, mailing, communicating, or conveying trade secrets. 18 U.S.C. § 1832(a)(2). The defendant must have acted "without

authorization" from the owner. Accordingly, an employee or licensee who has authorization to possess a trade secret during the regular course of employment violates the EEA if he or she transfers it without the owner's permission. *See* 142 Cong. Rec. S12,212 (daily ed. Oct. 2, 1996) ("authorization is the permission, approval, consent or sanction of the owner" to transfer a trade secret).

1. Knowledge: The government does not have to prove the defendant definitely knew the information was a trade secret. "For a person to be prosecuted, the person must know or have a firm belief that the information he or she is taking is proprietary." 142 Cong. Rec. S12,213 (daily ed. Oct. 2, 1996). Evidence that a defendant knew the owner marked the documents "confidential" or "proprietary," restricted access to the information, and required personnel to sign non-disclosure agreements is solid proof of this element. *Martin*, 228 F.3d at 12. A person who takes a trade secret because of ignorance, mistake, or accident, or who reasonably believes that the information is not proprietary, is not liable under the EEA.

2. Definition of a Trade Secret: The definition of a trade secret is broader under the EEA than under state civil statutes and the Uniform Trade Secrets Act, and includes both tangible property and intangible information. *Martin*, 228 F.3d at 11. It protects:

all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if –

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, or not being readily ascertainable through proper means by, the public.

---

18 U.S.C. § 1839(3). The EEA “protects a wider variety of technological and intangible information than current civil laws,” although “it is clear that Congress did not intend . . . to prohibit lawful competition such as the use of general skills or parallel development of a similar product.” *Hsu*, 155 F.3d at 196-97. Moreover, while the civil definition requires that the trade secret is not known by business people or competitors, the EEA’s definition requires only that the information not be known or ascertainable by the general public. *Id.*

An important issue at any trade secret trial is the owner’s effort to maintain the secrecy of the information. A non-exhaustive list of the relevant factors includes whether the owner:

- kept and enforced clear policies about the confidential information;
- trained its employees, consultants, and licensees regarding the proprietary information;
- required employees, consultants, and licensees to sign confidentiality and nondisclosure agreements;
- limited physical access to areas where the trade secrets were kept;
- restricted the number of copies of certain documents;
- kept hard copies of the documents on colored paper so they were difficult to photocopy;
- encrypted trade secrets kept in electronic form; and
- restricted access to certain electronic files and data on a “need to know” basis.

The owner’s security measures do not have to be absolute, but must be reasonable under the circumstances. 18 U.S.C. § 1839(3)(A). In addition, the information cannot be readily ascertainable through observation or reverse engineering.

Information disclosed to licensees, vendors, or third parties for limited purposes may still be a trade secret. *Rockwell Graphic Systems v. DEV Industries*, 925 F.2d 174, 177 (7th Cir. 1991).

Non-disclosure agreements can protect companies and retain the information’s trade secret status. Information can lose its status through legal filings and the issuance of a patent. However, refinements and enhancements of the technology set out in a patent may qualify as trade secrets if they are not reasonably ascertainable from the published patent. *United States v. Hsu*, 185 F.R.D. 192, 201 (E.D.Pa. 1999). The EEA’s definition of a trade secret is not unconstitutionally vague, although a district court has expressed concerns about determining what is “generally known” and “reasonably ascertainable.” *United States v. Hsu*, 40 F. Supp. 2d 623, 630 (E.D.Pa. 1999). According to the opinion,

what is ‘generally known’ and ‘reasonably ascertainable’ about ideas, concepts, and technology is constantly evolving in the modern age. With the proliferation of the media of communication on technological subjects, and (still) in so many languages, what is ‘generally known’ or ‘reasonably ascertainable’ to the public at any given time is necessarily never sure.

*Id.* The district court questioned whether information on the Internet or discussed at scientific conferences is readily ascertainable or generally known. *Id.*

The trade secret can be “minimally novel,” but some element must be unknown to the public. *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974). Not every part of the information needs to qualify as a trade secret, and a trade secret may include a combination of elements which are generally known to the public. “[A] trade secret can include a system where the elements are in the public domain, but there has been accomplished an effective, successful and valuable integration of the public domain elements and the trade secret gave the claimant a competitive advantage which is protected from misappropriation.” *Rivendell Forest Products v. Georgia Pacific Corp.*, 28 F.3d 1042, 1046 (10th Cir. 1994).

3. Independent Economic Value: The trade secret must derive “independent economic value . . . from not being generally known to . . . the

---

public.” 18 U.S.C. § 1839(3)(B). There is no minimum jurisdictional amount, however.

4. Economic Benefit to a Third Party: The government must prove that the theft was intended for the economic benefit of a person other than the rightful owner. A person who steals a trade secret but does not intend anyone to gain financially from the theft does not violate section 1832. This element is not included in section 1831. In section 1831, the benefit may be non-economic.

5. Intent to Injure the Owner: The government is not required to prove malice or evil intent, but only that the defendant knew or intended that the offense would injure the owner. *Hsu*, 155 F.3d at 196. Proof of a defendant’s plan to use the information to create a more successful competitor against the trade secret owner satisfies this element. *Martin*, 228 F.3d at 12.

6. Interstate or Foreign Commerce: The government must prove that the trade secret was “related to or included in a product that is produced for or placed in interstate or foreign commerce.” 18 U.S.C. § 1832. This term is not unconstitutionally vague. *Hsu*, 40 F. Supp. 2d at 627. The element should not be difficult to determine for products already in the marketplace. However, the element may be more problematic where the trade secrets relate to products in the development stage.

7. Customer lists: A customer list may be a trade secret under the EEA’s definition. In *Martin*, the First Circuit stated that a customer list “had the potential to fall within the § 1839 definition of trade secret.” *Martin*, 228 F.3d at 12 n.8. There, the evidence showed that the owner had devoted considerable resources generating and updating the lists, which included all of the relevant details about the customers in a defined and narrow market. However, customer lists are not trade secrets where they can be compiled by general marketing efforts, or where the base of customers is neither fixed nor small. *Nalco Chemical Co. v. Hydro Technologies*, 984 F.2d 801, 804 (7th Cir. 1993); *Standard Register Co. v. Cleaver*, 30 F. Supp. 2d 1084, 1095 (N.D. Ind. 1998).

8. Penalties: A person convicted under section 1832 can be imprisoned for up to ten years and fined \$250,000, and an organization can be fined up to \$5,000,000. 18 U.S.C. §§ 1832(a) and (b). The applicable guideline is USSG § 2B1.1. Calculating the loss is oftentimes difficult. In some cases, the value of the trade secret may be determined by what the defendant sought to pay for it, or by the cost of a legitimate licensing agreement. Value is far more difficult to determine when the information relates to a small part of a larger process, or the product to which the trade secret relates has not made it to the marketplace. The cost of the research and development for the information, and the “thieves market” theory are potential methods of determining the value.

Prosecutors should understand that the risk of divulging the trade secret may be greatest at the sentencing stage, as the nature of the trade secret is an important factor. Even under the Uniform Trade Secrets Act, courts have recognized that “the general law and the proper measure of damages in a trade secret case is far from uniform.” *Telex Corp. v. IBM*, 510 F.2d 894, 930 (10th Cir. 1975).

### **B. Section 1831: Foreign Economic Espionage**

Section 1831 was “designed to apply only when there is ‘evidence of foreign government sponsored or coordinated intelligence activity.’” *Hsu*, 155 F.3d at 195 (quoting 142 Cong.Rec. S12,212 (daily ed. Oct. 2, 1996)). Under section 1831, the government must prove that: (1) the defendant stole, or without the owner’s authorization obtained, destroyed, or conveyed information; (2) the defendant knew or believed that this information was a trade secret; (3) the information was a trade secret; and (4) the defendant intended or knew that the offense would benefit a foreign government, instrumentality, or agent. The term “foreign instrumentality” means “any agency, bureau, component, institution, association, or any legal, commercial, or business organization, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government.” 18 U.S.C. § 1839(1).

---

The legislative history reveals that, in this context, “substantial” means “material or significant, not technical or tenuous.” 142 Cong.Rec. S12,212 (daily ed. Oct. 2, 1996).

We do not mean for the test of substantial control to be mechanistic or mathematical. The simple fact that the majority of the stock of a company is owned by a foreign government will not suffice under this definition, nor for that matter will the fact that a foreign government only owns ten percent of a company exempt it from scrutiny. Rather, the pertinent inquiry is whether the activities of the company are, from a practical and substantive viewpoint, foreign government directed.

*Id.* The term “benefit” is to be interpreted broadly, and is not limited to economic gains. H.R. Rep. No. 788, 104th Cong. (1996).

Unlike section 1832, section 1831 does not require the government to prove that a defendant intended to convert the trade secret to the economic benefit of another, that the defendant intended or knew that the offense would injure the owner, or that the trade secret was related to a product in interstate or foreign commerce. The other proof elements have been discussed previously.

1. Extraterritoriality: Both sections 1831 and 1832 may control acts committed outside the country. The EEA applies if the offender is a citizen or resident alien of the United States, or an organization organized under the laws of the United States or any state. 18 U.S.C. § 1837.

2. Penalties: Congress imposed a greater penalty on those who steal trade secrets on behalf of foreign agents. A person convicted of violating section 1831 is subject to a term of imprisonment of up to 15 years and a fine of \$500,000. 18 U.S.C. § 1831(a). An organization convicted under section 1831 faces a fine of not more than \$10,000,000. *Id.* at § 1831(b).

## II. Conspiracies

The EEA prohibits conspiracies to steal trade secrets. In order to prevail, the government must prove: (1) that an agreement existed; (2) that it

had an unlawful purpose; (3) that the defendant was a voluntary participant; (4) that the defendant possessed both the intent to agree and the intent to commit the substantive offense; and (5) that at least one co-conspirator took an affirmative step toward achieving the conspiracy’s purpose. *Martin*, 228 F.3d at 11; *Hsu*, 155 F.3d at 202. It is irrelevant whether the defendant actually received a trade secret. *Martin*, 228 F.2d at 13. It is sufficient to prove that the conspirators agreed to convey information “that potentially fell under the definition of a trade secret in 18 U.S.C. § 1839.” *Id.* Legal impossibility is not a defense to a conspiracy charge. *Hsu*, 155 F.3d at 203. Prosecutors should recognize the advantages of charging conspiracy wherever possible, as there are fewer elements to prove and there is a reduced risk the trade secrets will be disclosed during the litigation.

## III. Preserving Confidentiality of Trade Secrets During Litigation

Congress recognized the practical problem faced in all trade secret cases – litigation to protect the trade secret could actually lead to the disclosure of the trade secret during the course of the trial. A defendant who has tried to obtain trade secrets by stealth and fraud might, after indictment, gain access to the same information through the federal discovery rules. Congress wanted to protect trade secrets during the litigation without infringing upon a defendant’s rights, so it included a provision directing that a court “shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirement” of the applicable federal rules and laws. 18 U.S.C. § 1835. This confidentiality provision “represent[s] a clear indication from Congress that trade secrets are to be protected to the fullest extent during EEA litigation.” *Hsu*, 155 F.3d at 197. The confidentiality provision was also intended to encourage victims to report thefts, as it provides some assurance that the trade secret will not be divulged during the litigation. *Id.*

The *Hsu* case is instructive. There, the indictment charged that the defendants contacted an FBI agent posing as a technological

---

information broker and directed him to purchase information about an anti-cancer drug. *Hsu*, 155 F.3d at 192. The undercover agent announced that he had found a corrupt employee of the drug manufacturer, and arranged a meeting with the defendants. *Id.* At that meeting, the supposedly corrupt employee showed company documents which contained trade secrets and were marked “confidential.” *Id.* at 192-93. As part of discovery, the defense requested a copy of the documents shown to the defendants during the meeting. *Id.* at 193. The trial court adopted the defendant’s proposal that the proprietary information would only be disclosed to select members of the defense team, and any documents filed with the court containing the information would remain under seal. *Id.* at 193. The trial court also encouraged the government to file an interlocutory appeal, as permitted under section 1835. *Id.* at 194. The Third Circuit reversed, holding that the defendant should not obtain access to the trade secrets because they were only charged with conspiring to violate the EEA. *Id.* at 199. The Circuit Court reasoned that because impossibility is not a defense to the conspiracy charge, whether the documents contained actual trade secrets and the nature of the trade secrets themselves were irrelevant. *Id.*

At a minimum, prosecutors should require the defendant, counsel, and any experts retained by the defendant to sign confidentiality agreements protecting all proprietary information. Federal prosecutors and law enforcement agencies do not need to sign protective orders with victims before accepting trade secret information, however. 18 U.S.C. § 1833.

The government may file an interlocutory appeal from an order authorizing or directing the disclosure of trade secrets. 18 U.S.C. § 1835. Since delaying the trial during an interlocutory appeal will usually help only the defendant, prosecutors should ensure that there are procedures in place to limit the chance that actual trade secrets will be discussed in open court. Prosecutors can more readily restrict disclosure when they charge a defendant only with conspiring or attempting to steal trade secrets, since the government does not have to prove that the information was actually a trade secret. *Hsu*,

155 F.3d at 203-04. In fact, in attempt and conspiracy cases, the government might not even offer in evidence any documents containing actual trade secrets. Department guidelines require the Deputy Attorney General’s approval before a federal prosecutor can request that a courtroom be sealed. *See* 28 C.F.R. § 50.9; *U.S. Attorney’s Manual* § 9-5.150.

#### **IV. Forfeiture**

The EEA provides that a court “shall” order the forfeiture of any proceeds or property derived from the violation, and may order the forfeiture of any property used to commit or facilitate the commission of the crime, “taking into consideration the nature, scope, and proportionality of the use of the property in the offense.” 18 U.S.C. § 1834(a). With certain exceptions, the procedures set out in 21 U.S.C. § 853 govern the forfeiture proceedings.

#### **V. Department of Justice Oversight**

Responding to Congressional concerns that prosecutors might misapply the EEA, the Department of Justice agreed to require that all prosecutions under the EEA must first be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General of the Criminal Division. 28 C.F.R. § 0.64-5. This regulation, which remains in effect until October 11, 2001, applies to the filing of complaints, indictments, and informations, but not to search warrant applications. The Computer Crime and Intellectual Property Section (“CCIPS”) coordinates requests for approval of cases under section 1832. In cases involving charges under section 1831, CCIPS consults with the Internal Security Section.

#### **VI. Conclusion**

It is hard to overstate the threat posed by the theft of proprietary information. The Computer Security Institute stated recently that “theft of proprietary information is perhaps the greatest threat to United States economic competitiveness in the global marketplace.” The theft of trade secrets can affect any economic sector; high tech companies are not the only ones concerned about somebody stealing their trade secrets. *See Shurgard Storage Centers v. Safeguard Self*

---

*Storage*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (in civil action, plaintiff alleged that defendant systematically hired key employees away for purpose of obtaining plaintiff's trade secrets). As the workforce becomes ever more mobile, and as other countries strive to compete by any means necessary, the threat will persist. The EEA provides prosecutors with an effective tool to combat this threat from whatever source – a sophisticated foreign agency or an unhappy employee like Caryn Camp.

#### ABOUT THE AUTHOR

**Toby Dilworth** graduated from Yale University and Boston College Law School with honors. After serving as a law clerk for U.S. District Judge Gene Carter, he joined a private firm in Portland, Maine. He became an Assistant United States Attorney for the District of Maine in 1991. He now serves as the Computer and Telecommunications Coordinator in the Portland office. He is also an adjunct faculty member at the University of Maine Law School, where he teaches trial practice. [a](#)

---

## It's Not Just Fun and "War Games" – Juveniles and Computer Crime

*Joseph V. DeMarco*  
*Assistant United States Attorney*  
*Southern District of New York*  
*Computer and Telecommunications Coordinator*

### I. Introduction

In the 1983 movie "War Games," Matthew Broderick and Ally Sheedy play high school students who inadvertently access the NORAD computer network, thinking that they are merely playing a "war game" with the computers. As a consequence, Broderick and Sheedy come Hollywood-close to initiating a nuclear exchange between the United States and the Soviet Union. In order to accomplish this hack, Broderick configures his PC's modem to automatically dial random telephone numbers in the city where the computers he hopes to break into are located. When Sheedy asks Broderick how he pays for all the telephone calls, Broderick coyly tells her that "there are ways around" paying for the phone service. Sheedy asks: "Isn't that a crime"? Broderick's reply: "Not if you are under eighteen."

This article demonstrates why Broderick was wrong, for, while the movie may have seemed to

be pure science fiction, the increased reliance on computers at all levels of society, coupled with the explosive growth in the use of personal computers and the Internet by teens, has made the scenario portrayed by the film seem to be not so fictional. Consider the following cases:

- C A juvenile in Massachusetts pleads guilty to charges he disabled a key telephone company computer servicing the Worcester airport control tower, thereby disabling both the main radio transmitter, as well as a circuit which enabled aircraft on approach to send signals activating the runway lights.
- C A 16-year-old from Florida pleads guilty and is sentenced to six months in a detention facility for intercepting electronic communications on military computer networks and for illegally obtaining information from a NASA computer network.
- C A 16-year-old in Virginia pleads guilty to computer trespassing after hacking into a Massachusetts Internet service provider's (ISPs) computer system, causing \$20,000 in damages.

---

C A 13-year-old California boy pleads guilty to making threats directed against a 13-year-old girl over the Internet. The boy had created a website which included a game featuring the girl's picture over a caption which read: "Hurry! Click on the trigger to kill her." The website included a petition calling for the girl's death.

See [www.cybercrime.gov/juvenilepld.htm](http://www.cybercrime.gov/juvenilepld.htm) (Worcester airport); [cybercrime.gov/comrade.htm](http://cybercrime.gov/comrade.htm) (NASA case) Arthur L. Bowker, *Juveniles and Computers: Should We Be Concerned*, Federal Probation, December 1999, at 40 (Virginia and California cases) .

This article seeks to explain: (1) why and how the rise of the computer culture and Internet generation presents opportunities for juveniles to commit crimes distinctly different from those traditionally committed by minors; (2) the statutory framework governing prosecution of computer delinquents in federal court; and (3) special considerations which pertain to the prosecution of computer crimes by juveniles. At a time when a *Newsweek* survey estimates that almost eighty percent of children regularly go online, the incidence of computer crime committed by juveniles will, increasingly, come to a prosecutor's attention.

## II. Kids and Computer Crime

As has been documented in other articles in this publication, the rapid growth in the use of personal computers (PCs) and the advent of the Internet have made it possible for persons of all ages to commit serious crimes – including extortion, computer hacking, and credit card fraud – without ever leaving the comfort of home. In addition, difficulties in obtaining electronic evidence and tracing back to the electronic wrongdoer present unique challenges to law enforcement investigating computer crimes committed by persons of any age. In the context of juveniles who engage in criminally antisocial computer behavior, these problems take on special significance. This is true for several reasons.

First, the enormous computing power of today's PCs make it possible for minors to commit offenses which are disproportionately

serious to their age. For example, while property offenses committed by minors in the "brick and mortar" world typically include shoplifting or other forms of simple theft, the advent of computer technology has made it possible for minors in the "point and click" world to engage in highly complex fraud schemes. "Typical" computer crimes committed by minors include trading stolen credit card numbers and amassing thousands of dollars worth of fraudulent purchases on those cards, or large-scale pirating of copyrighted computer software which is later sold or bartered to other minors in exchange for other pirated software. A Canadian juvenile has already been held responsible for launching a massive denial of service attack costing American companies millions of dollars. Likewise, there is, in principle, no reason why a juvenile could not release a computer virus, infecting tens of thousands of computers, or engage in large scale securities manipulation, causing six and seven-figure damages to investors. Indeed, given the technological sophistication of today's youth (evident to any parent who has relied on their fourteen year-old to set up the family computer), it is possible for a teenager to commit computer-related property offenses on a scale to which, prior to the 1980's, only seasoned veterans of the criminal justice system could aspire.

Second, the ability of a juvenile to portray himself or herself as an adult in the online world means that juveniles have access to fora in which to engage in criminal activity – for example, auction Websites, financial services Websites, and chat rooms – that in the physical world would quickly deny them any access at all. This access opens doors to criminality previously closed to minors. In a similar vein, kids who are too young to drive can use a PC connected to the Internet to access computers worldwide, adding to their ability to commit serious and far-reaching offenses and to confederate with other computer delinquents. Not only is it difficult for parents to deny their children access to computers – necessary for much legitimate schoolwork – even were parental control at home practicable, the ubiquitous (and often free) computer access provided by high schools, public libraries, and friends make "computer curfews" an oxymoron.

---

Third, juveniles appear to have an ethical "deficit" when it comes to computer crimes. In one study, 34 percent of university undergraduates admitted to illegally pirating copyrighted software, and 16 percent admitted to gaining illegal access to a computer system to browse or exchange information. *See* Bowker, *Juveniles and Computers*, at 41 (citing surveys). Moreover, a recent poll of 47,235 elementary and middle school students conducted by Scholastic, Inc. revealed that 48% of juveniles do not consider hacking to be a crime. This ethical deficit increases the likelihood that even "good kids" who are ordinarily unlikely to commit crimes such as robbery, burglary, or assault, may not be as disinclined to commit online crimes.

### III. Prosecuting Juveniles in Federal Court

Against this backdrop, Federal prosecutors bringing computer delinquents to justice must master the provisions of the criminal code applicable to those actions. Specifically, they must understand the Juvenile Justice and Delinquency Prevention Act (the "Act"), codified at 18 U.S.C. §§ 5031 to 5042 of Title 18, which governs both the criminal prosecution or the delinquent adjudication of minors in federal court. While a complete analysis of the Act is beyond the scope of this article, certain of its provisions bear discussion, for proceedings against juveniles in federal court differs in significant respects from the prosecution of adults, and the prosecution of computer delinquents presents special considerations different from juveniles involved in other delinquencies. Specifically, as described below, the Act creates a unique procedure for delinquency proceedings against juveniles – a process quasi-criminal and quasi-civil in nature, replete with its own procedural complexities and particular rules. In their totality, these unique provisions seek to take account not only of the special protections provided to minors but also of the fact that even persons under 18 can commit "adult" crimes.

As a threshold matter, it is important to note that a juvenile proceeding is not the same as a criminal prosecution. Rather it is a proceeding in which the issue to be determined is whether the minor is a "juvenile delinquent" as a matter of

status, not whether he or she is guilty of committing a crime. Thus, a finding against the juvenile does not result in a criminal conviction; instead, it results in a finding of "delinquency." Indeed, the juvenile proceeding is specifically designed to *lessen* the amount of stigma that attaches to the act of delinquency compared to a criminal conviction, and to emphasize the rehabilitation, rather than punishment, of the juvenile. *See, e.g., United States v. Hill*, 538 F.2d 1072, 1074 (4th Cir. 1976). With that background in mind, several aspects of the Act can be examined.

#### A. Who Is A Juvenile?

Under the Act, a "juvenile" is a person who has not yet reached the age of eighteen at the time of the commission of the offense *and* is under twenty one as of the time of the filing of formal juvenile charges. *See* 18 U.S.C. § 5031. Thus, a person who committed the offense before his eighteenth birthday but is over twenty one on the date formal charges are filed may be prosecuted as an adult; the juvenile delinquency proceedings do not apply at all. This is true even where the government could have charged the juvenile prior to his twenty-first birthday but did not. *See In re Jack Glenn Martin*, 788 F.2d 696, 698 (11th Cir. 1986) (determinative date is date of filing of formal indictment or information, fact that Government could have brought charges against defendant prior to his twenty-first birthday held to be "irrelevant"); *see also United States v. Hoo*, 825 F.2d 667 (2d Cir. 1987) (absent improper delay by government, age at time of filing of formal charges determines whether the Act applies).

#### B. Does Federal Jurisdiction Exist?

As is true in the case of adults, not every criminal act violates federal law. Only where Congress has determined that a particular federal interest is at stake, and has passed appropriate legislation, can a federal criminal prosecution go forward. In general, under the Act, there are three situations where federal delinquency jurisdiction over a juvenile exists. *First*, where the state court lacks jurisdiction, or refuses to assume jurisdiction. *See* 18 U.S.C. § 5032. *Second*, where the state does not have available programs and

---

services adequate for the needs of juveniles. *See id.* *Third*, where the crime is a federal felony crime of violence or one of several enumerated federal offenses (principally relating to narcotics and firearm offenses), and there exists a sufficient federal interest to warrant exercise of federal jurisdiction. *See id.* These three jurisdictional bases are discussed below.

1. No State Statute, or State Refuses Jurisdiction: This first basis for federal jurisdiction will be the most frequently used basis in the context of juvenile computer delinquents. It encompasses situations where a state has no law criminalizing the specific conduct, or does have a law but, for whatever reason, indicates that it will not pursue a proceeding under its law against the minor. With regard to the former, although many states have enacted laws analogous to the general federal computer crime statute (18 U.S.C. § 1030), the electronic eavesdropping statute (18 U.S.C. § 2511), and the access device fraud statute (18 U.S.C. § 1029), to pick the most commonly prosecuted cybercrimes, some states do not have laws under which the crime in question can be prosecuted. In these cases, under the Act, the juvenile, nevertheless, can be held to account for his or her act of delinquency under federal law.

More commonly, however, a state will have a statute which does cover the cybercrime in question, *see, e.g.*, N.Y. Penal Law § 156.10 (computer trespass); *id.* § 156.27 (computer tampering in the first degree); *id.* § 250.05 (intercepting or accessing electronic communications), but will be unwilling to assume jurisdiction over the juvenile, perhaps because of a shortage of resources, or a dearth of technical and/or prosecutorial expertise. In such cases, upon certification by the United States Attorney that pertinent state officials do *not* wish to proceed against the juvenile, the Federal Government may assume jurisdiction. *See* 18 U.S.C. § 5032.

In the context of cybercrime, certain offenses committed by juveniles may amount to crimes in multiple states. A crippling denial-of-service-attack or the transmission of a computer virus can generate victims in numerous jurisdictions. The Act, however, does not appear to require that, in

such cases, the government must certify that each and every state that could potentially have jurisdiction is unwilling to assume the jurisdiction at their disposal. The Act merely requires that the "juvenile court or other appropriate court of a State does not have jurisdiction or refuses to assume jurisdiction over [the] juvenile." 18 U.S.C. § 5032 (emphasis supplied). Typically, the pertinent state will be the state contemplating proceedings against the minor which, in practice, will often be the state in which the federal prosecutor investigating the case sits. Of course, since federal criminal proceedings can often preclude state criminal proceedings under state double jeopardy principles, federal prosecutors faced with multi-state cases should consult with prosecutors from all affected states in order to determine what, if any effect, a federal juvenile proceeding may have on a state's proceedings. Consultation is also warranted because certain states may provide for treatment of the juvenile as an adult more easily than the provisions of the Act (discussed below) which deal with transfer of a juvenile to adult status.

2. The State Has No Programs or Inadequate Programs: This second basis for federal jurisdiction arises infrequently, as most states do have programs and facilities which provide for the adjudication, detention, and rehabilitation of minors. (Indeed, as of the writing of this article, there are no federal detention facilities specifically designed for juveniles. Juveniles who are the subject of federal delinquency proceedings are housed in contract facilities run by state, local, or private entities.) However, in the event that state officials were, for any reason, unable to address the needs of a juvenile, this exception would apply.

3. Enumerated Crimes and Crimes of Violence: Finally, the Act also sets forth certain federal crimes for which jurisdiction is deemed to exist, and where there is a substantial federal interest to warrant jurisdiction. The enumerated offenses are controlled substance offenses arising under 21 U.S.C. §§ 841, 952(a), 953, 955, 959, 960(b)(1), (2), (3), as well as firearms-related offenses arising under 18 U.S.C. §§ 922(x), 924(b), (g), or (h). While these offenses are typically inapplicable to cybercrime, the statute

---

also permits jurisdiction in cases of "crimes of violence" which are punishable as felonies. *See* 18 U.S.C. § 5032. Although the Act itself does not define it, 18 U.S.C. § 16 defines crimes of violence as offenses that "ha[ve] as an element the use, attempted use, or threatened use of physical force against the person or property of another," or any offense "that is a felony and that, by its nature, involves a substantial risk that physical force against the person or property of another may be used in the commission of committing the offense." 18 U.S.C. § 16. In the context of cybercrime, the statutes which implicate this basis of jurisdiction include 18 U.S.C. § 875(b) (transmission in interstate or foreign commerce of extortionate threats to injure another person), 18 U.S.C. § 1951(a) and (b)(2) (interference with commerce by extortion or threats of physical violence), and 18 U.S.C. § 844(e) (transmission of, *inter alia*, bomb threats).

Prosecutors relying on this third basis for jurisdiction should keep in mind that their certification must not only set forth a federal felony crime of violence, but must also certify that a substantial federal interest in the case or offense warrants assumption of federal jurisdiction. Eight of the nine circuits that have addressed the issue have held that the United States Attorney's certification of a substantial federal interest is not subject to appellate review for factual accuracy; only the Fourth Circuit has held otherwise. *See United States v. John Doe*, 226 F.3d 672, 676-78 (6th Cir. 2000) (collecting cases).

Where the Federal Government is the victim of a crime, the federal interest is apparent. Yet, even when it is not the victim, federal interests often exist, as cybercrime often involves conduct affecting critical infrastructures (*e.g.*, telecommunications systems); industries, or technologies significant to the nation's economy (*e.g.*, aerospace, computer software); or criminal groups operating in multiple states and/or foreign countries (*e.g.*, identity theft and stolen credit card rings). It is precisely in these important and often hard-to-enforce-locally situations that federal jurisdiction is peculiarly appropriate.

### C. Delinquency Proceedings

Assuming that federal juvenile jurisdiction exists, prosecutors bringing such actions will typically commence the action with the filing, under seal, of a juvenile information and the jurisdictional certification. *See* 18 U.S.C. § 5032, ¶¶ 2-3. It is important to note that the certification must be signed by the United States Attorney personally, and a copy of the pertinent memorandum delegating authority from the Assistant Attorney General to the United States Attorneys to sign the certification should be attached to the submission. (A copy of the delegation memorandum, dated July 20, 1995, can be obtained from the Terrorism and Violent Crime Section of the Department of Justice.)

A juvenile has no Fifth Amendment right to have his or her case presented to a grand jury, nor does the juvenile have the right to a trial by jury. *See, e.g., United States v. Hill*, 538 F.2d 1072, 1075-76 (4th Cir. 1976); *United States v. Indian Boy*, 565 F.2d 585, 595 (9th Cir. 1975). Instead, the "guilt" phase of a delinquency proceeding is essentially conducted as a bench trial. And in that trial – in which the government must prove that the juvenile has committed the act of delinquency beyond a reasonable doubt – the juvenile has many of the same rights as a criminal defendant. These include: (1) the right to notice of the charges; (2) the right to counsel; (3) the right to confront and cross-examine witnesses; and (4) the privilege against self-incrimination. *See Hill*, 538 F.2d at 1075, n.3 (collecting cases). Moreover, in the delinquency proceeding, the Federal Rules of Criminal Procedure apply – to the extent their application is not inconsistent with any provision of the Act. *See* Fed. R. Crim. P. 54(b)(5); *see also* Wright, *Federal Practice and Procedure: Criminal 2d* § 873. The Federal Rules of Evidence likewise apply to the delinquency trial, *see* F.R.E. 101, 1101, although courts have held them inapplicable to transfer proceedings, discussed below. *See Government of the Virgin Islands in the Interest of A.M., a Minor*, 34 F.3d 153, 160-62 (3rd Cir. 1994) (collecting cases).

In addition, the Act affords juveniles special protections not ordinarily applicable to adult defendants. Most notably, the juvenile's identity is

---

to be protected from public disclosure. *See* 18 U.S.C. § 5038 (provisions concerning sealing and safeguarding of records generated and maintained in juvenile proceedings). Thus, court filings should refer to the juvenile by his or her initials and not by name, and routine booking photographs and fingerprints should not be made or kept. Moreover, whenever a juvenile is taken into custody for an alleged act of delinquency, the juvenile must be informed of his or her legal rights "in language comprehensible to [the] juvenile," 18 U.S.C. § 5033, and the juvenile's parent, guardian, or custodian must be notified immediately of the juvenile's arrest, the nature of the charges, and the juvenile's rights. *Id.* Upon arrest, the juvenile may not be detained for longer than a reasonable period of time before being brought before a magistrate. *Id.* When brought before a magistrate, the juvenile must be released to his or her parents or guardian upon their promise to bring the juvenile to court for future appearances, unless the magistrate determines that the detention of the juvenile is required to secure his or her appearance before the court, or to insure the juvenile's safety or the safety of others. *See* 18 U.S.C. § 5034. At no time may a juvenile who is under twenty one years of age and charged with an act of delinquency or adjudicated delinquent be housed in a facility where they would have regular contact with adults. *See* 18 U.S.C. §§ 5035, 5038. Under the Act, a juvenile has a right to counsel at all critical stages of the proceeding, and the Act authorizes the appointment of counsel where the juvenile's parents or guardians cannot afford to retain counsel. *Id.*

#### **D. Transfers From Juvenile Delinquency Proceedings To Adult Criminal Proceedings**

As noted above, under certain circumstances, a juvenile's case may be transferred to adult status and the juvenile can be tried as an adult. In these situations, the case proceeds as any criminal case would with the exception that a juvenile under eighteen who is transferred to adult status may never be housed with adults, either pretrial or to serve a sentence. Most notably, a juvenile may transfer to adult status by waiving his juvenile status, upon written request and advice of counsel. *See* 18 U.S.C. § 5032, ¶4. In addition, the Act creates two forms of transfer which do not take

into account the juvenile's wishes: discretionary transfer and mandatory transfer.

As the name implies, discretionary transfer is an option available, upon motion by the Government, in certain types of cases where the juvenile is age fifteen or older at the time of the commission of the act of delinquency. *See* 18 U.S.C. § 5032, ¶4. As applied to the field of cyber-delinquency, it is available in cases involving felony crimes of violence (*e.g.*, extortion, bomb threats). Under the Act, a court must consider six factors in determining whether it is in the interest of justice to grant the Government's motion for discretionary transfer: (1) the age and social background of the juvenile; (2) the nature of the alleged offense, including the juvenile's leadership role in a criminal organization; (3) the nature and extent of the juvenile's prior delinquency record; (4) the juvenile's present intellectual development and psychological maturity; (5) the juvenile's response to past treatment efforts and the nature of those efforts; and (6) the availability of programs to treat the juveniles behavioral problems. *See* 18 U.S.C. § 5032, ¶5. In the context of typical computer crimes committed by juveniles several of the factors will often counsel in favor of transfer to adult status: many cyber-delinquents come from middle-class, or even affluent backgrounds; many commit their exploits with the assistance of other delinquents; and many are extremely intelligent. Moreover, many of the most sophisticated computer criminals are under eighteen by only a few months and, as verge-of-adult wrongdoers, may well merit adult justice.

Mandatory transfer is more circumscribed than discretionary transfer, and is limited to certain enumerated offenses (*e.g.*, arson) which are not typically applicable in cyber-prosecutions, or to violent felonies directed against other persons. *See* 18 U.S.C. § 5032, ¶4. Here, however, transfer is further limited to offenses committed by juveniles age sixteen and older who also have a prior criminal conviction or juvenile adjudication for which they could be subject to mandatory or discretionary transfer. As a practical matter, therefore, in the area of cybercrime the majority of proceedings begun as juvenile proceedings will

---

likely remain as such, and will not be transferred to adult prosecutions.

### **E. Sentencing And Detention**

Under the Act, a court has several options in sentencing a juvenile adjudged to be delinquent. The court may suspend the finding(s) of delinquency; order restitution; place the juvenile on probation; or order that the juvenile be detained. *See* 18 U.S.C. § 5037(a). In cases where detention is ordered, such detention can never be longer than the period of detention the juvenile would have received had they been an adult. *See* 18 U.S.C. § 5037(b). Accordingly, the Sentencing Guidelines, although not controlling, must be consulted. U.S.S.G. § 1B1.12; *see United States v. R.L.C.*, 503 U.S. 291, 307 n.7 (1992). Finally, if the disposition hearing is before the juvenile's eighteenth birthday, he or she may be committed to official detention until his or her twenty-first birthday or the length of time they would have received as an adult under the Sentencing Guidelines, whichever term is less. If the juvenile is between eighteen and twenty-one at the time of the disposition, he or she may be detained for a maximum term of three or five years (depending on the type of felony relevant to the proceeding), but in no event can he or she be detained longer than they would be as an adult sentenced under the Guidelines. *See* 18 U.S.C. § 5037(b), (c).

### **IV. Special Considerations**

As demonstrated above, federal delinquency proceedings are unique from a legal point of view, and prosecutors initiating such proceedings would do well to consult closely with the United States Attorney's Manual provisions concerning delinquency proceedings, *see* USAM § 9-8.00, as well as the Terrorism and Violent Crime Section (TVCS), which serves as the Department's expert in this field. Prosecutors should also familiarize themselves with the legal issues typically litigated in this area in order to avoid common pitfalls. *See, e.g.,* Jean M. Radler, Annotation, *Treatment Under Federal Juvenile Delinquency Act (18 U.S.C. §§ 5031-5042) Of Juvenile Alleged To Have Violated Law of United States*, 137 ALR Fed. 481 (1997).

In addition to the novel nature of the proceedings themselves, however, crimes committed by juveniles pose unique investigative challenges. For example, common investigative techniques such as undercover operations and the use of cooperators and informants can raise difficult issues rarely present in the investigations of adults. Indeed, a seemingly routine post-arrest interview may raise issues of consent and voluntariness when the arrestee is a juvenile which are not present in the case of an adult arrestee. *Compare, e.g., United States v. John Doe*, 226 F.3d 672 (6th Cir. 2000) (affirming district court's refusal to suppress juvenile's confession notwithstanding arresting officer's failure to comply with parental notification provisions of Act, where circumstances surrounding confession demonstrated voluntariness of juvenile's confession) *with United States v. Juvenile (RRA-A)*, 229 F.3d 737 (9th Cir. 2000) (ruling that juvenile's confession should be suppressed where arresting officer's failure to inform parents may have been a factor in confession, notwithstanding juvenile's request to arresting officers that her parent's *not* be contacted and informed of the arrest).

Alternatively, consider the case of a juvenile in a foreign country who, via the Internet, does serious damage to a United States Government computer or to an e-commerce Webserver. Ordinarily, of course, extradition of foreign nationals to the United States is governed by treaty. Where they exist, treaties generally fall into two categories: "dual criminality" treaties, in which the signatories agree to extradite for offenses if the offenses are criminal in both nations, and "list" treaties, in which extradition is possible only for offenses enumerated in the treaty. Interestingly, however, some extradition treaties contain provisions which specifically permit the foreign sovereign to take account of the youth of the offender in deciding whether to extradite. *E.g.,* Convention on Extradition between the United States of America and Sweden, 14 UST 1845; TIAS 5496 (as supplemented by Supplementary Convention on Extradition, TIAS 10812). How these international juvenile delinquency situations will unfold in the future is unclear. What is clear is

---

that as more and more of the planet becomes "wired," opportunities for cybercrime – including cybercrime by juveniles – will only increase. (Prosecutors who encounter situations involving juvenile's operating from abroad should, in addition to consulting with TVCS, consult with the Department's Office of International Affairs.)

#### V. Conclusion

Whether investigating a juvenile who commits a cybercrime involving computers maintained by a private party or computers maintained by segments of the strategic triad, a prosecutor considering bringing a juvenile to justice must not

only master a new area of law, but also must be aware that traditional approaches to a case bear reevaluation in light of the unique aspects and special considerations presented by a juvenile who engages in acts of cyber-delinquency.

#### ABOUT THE AUTHOR

**Joseph V. De Marco** is an Assistant United States Attorney for the Southern District of New York, where he serves as Computer and Telecommunications Coordinator. Currently, he is on detail to the Department's Computer Crimes and Intellectual Property Section in Washington, D.C. **a**

---

# The Computer and Telecommunications Coordinator (CTC) Program

*Stacey Levine*  
*Trial Attorney*  
*Computer Crime and Intellectual Property Section*

In 1995, at the recommendation of the then-Computer Crime Unit (now the Computer Crime and Intellectual Property Section (CCIPS)), the Department of Justice created the Computer and Telecommunication Coordinator (CTC) Program to protect the nation's businesses and citizens from the rising tide of computer crime. The CTC program has now grown to 137 attorneys. Each United States Attorney's Office (USAO) has designated at least one CTC and over thirty-five districts have two or more. In addition, a number of Sections in the Criminal Division and other Divisions of Justice also have designated CTCs. The CTCs have four general areas of responsibility:

**1. Prosecuting Computer Crime:** At a yearly conference organized by CCIPS and at other times, the CTCs receive special training and

periodic updates concerning legal and technical issues involved in investigating and prosecuting cybercrime, such as hacking, child pornography, theft of intellectual property and fraud. To ensure that these cases are effectively prosecuted, the CTCs must have a thorough grasp of the technology and vocabulary involved in these types of cases. Moreover, in the preparation of direct and cross-examination of expert witnesses at trial, it is necessary for the CTC to achieve a fairly high level of understanding of the technology and the operating systems that are the subject of the litigation. To date, the CTCs have prosecuted a number of high-profile cases in the computer crime arena.

For example, in *United States v. Smith*, CR- No. 99-730(JAG) (D.N.J. Guilty Plea Entered December 9, 1999), a CTC in the United States Attorney's Office in New Jersey, with the aid of an attorney from CCIPS, charged David Smith with violating 18 U.S.C. 1030(a)(5)(A) for disseminating the Melissa virus. Smith pleaded

---

guilty to the offense and stipulated that his virus caused over \$80 million in computer damages.

In *United States v. Kevin Mitnick*, 145 F.3d 1342 (9th Cir. 1998) available at 1998 WL255343, the defendant was indicted for multiple counts of wire fraud, computer fraud, illegal possession of access devices and illegal interception of wire communications stemming from his systematic intrusions and theft of millions of dollars of proprietary information from many of the world's largest cellular phone and computer software manufacturers. The case was prosecuted by CTCs in Los Angeles in coordination with CTCs in San Francisco, the Eastern District of North Carolina and numerous other districts where Mitnick engaged in computer hacking and theft. Mitnick pleaded guilty and was sentenced to a total of 68 months incarceration.

The CTCs have also been actively pursuing thefts of intellectual property. For example, in *United States v. Jing Jing Fan Mou*, CR-00-504-R (C.D. Cal. Sentenced Dec. 4, 2000), a case handled by the CTC in the Central District of California, the defendant was charged with operating a trafficking ring that purchased and distributed Microsoft software worth over \$600,000. The defendant was sentenced to a year in prison and ordered to pay restitution to Microsoft.

**2. Technical Advisor:** The CTC also serves as a technical advisor and resident counsel to his or her fellow prosecutors in the USAO on high-tech issues. By staying current in the field, the CTC is able to assist his or her office not only in cases concerning crimes against information technology but also in those cases involving electronic search and seizures or related issues.

**3. Liaison:** Network crimes do not recognize borders that separate countries, much less judicial districts. Therefore, CTCs often become involved in investigations with victims in different jurisdictions and perishable evidence housed by Internet Service Providers (ISPs) located around the country or the world. Usually, the location of a perpetrator, if it ever can be established, can only be ascertained at the end of an investigation, and may involve a different location altogether. Thus, to function well as a CTC, an AUSA must be

prepared to work quickly and effectively to obtain orders for perishable evidence when asked to do so by a fellow CTC or CCIPS. The CTC may be asked to spend a great deal of time and effort on a case that may not result in an indictment or a prosecution in his or her district. Without this network of cooperation, it would be impossible to effectively investigate and prosecute these crimes.

**4. Training and Outreach:** One of the core duties of the CTC is to provide training and guidance to other AUSAs and to federal and local agencies in their district. By instructing federal, state, and local agents and prosecutors on searching and seizing computers, obtaining electronic evidence, and other issues, the CTCs help to ensure that law enforcement obtains admissible evidence and remains within the parameters set by the U.S. Constitution and Congress. The CTC should also establish relationships with regional experts from educational institutions and the technology industry to encourage open communication in the event of a computer intrusion or other network crime. These groups can also help the CTC to strengthen federal technical expertise in their districts.

For more information on the work of the CTCs and CCIPS, please visit [www.cybercrime.gov](http://www.cybercrime.gov).

#### ABOUT THE AUTHOR

**Stacey Levine** is a trial attorney in the Computer Crime and Intellectual Property Section. Prior to this, she was an Assistant United States Attorney in the Southern District of Florida. Before joining the Department of Justice she clerked for the Honorable Edward B. Davis, United States District Court, Southern District of Florida. 

## UPCOMING PUBLICATIONS

July 2001 Tax Issues

## Request for Subscription Update

In an effort to provide the UNITED STATES ATTORNEYS' **BULLETIN** to all who wish to receive it, we are requesting that you e-mail Nancy Bowman ([nancy.bowman@usdoj.gov](mailto:nancy.bowman@usdoj.gov)) with the following information: Name, title, complete address, telephone number, number of copies desired, and e-mail address. If there is more than one person in your office receiving the **BULLETIN**, we ask that you have one receiving contact and make distribution within your organization. **NOTE: We address our mailing labels with titles only.** If you do not have access to e-mail, please call 803-544-5158. Your cooperation is appreciated.