March
2014
Volume 62
Number 2

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

H. Marshall Jarrett
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 bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

Managing Editor
Jim Donovan

Associate Editor
Carmel Matin

Law Clerk
Jennifer Jokerst

Internet Address
www.usdoj.gov/usao/reading_room/foiamanuals.html

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

Cyber-Investigative Issues II

In This Issue

The Flood Tide of Cyberfraud

Jonathan J. Rusch
Deputy Chief for Strategy and Policy
Fraud Section
Criminal Division

Cyberfraud, also known as online fraud or Internet fraud, can be defined simply as "the use of the internet to get money, goods, etc. from people illegally by deceiving them." CAMBRIDGE DICTIONARIES ONLINE, http://dictionary.cambridge.org/us/dictionary/british/cyberfraud. Over the past decade, as the World Wide Web has become increasingly indispensable for global communication and commerce, cyberfraud has become a flood tide that poses significant threats to individuals and businesses around the world.

I. Incidence and prevalence of cyberfraud

There are no comprehensive measures of cyberfraud worldwide. Various surveys and reports, however, provide some indications of its incidence and prevalence. The 2014 Identity Fraud Report by a private-sector research firm, Javelin Strategy & Research, found that the incidence of fraud involving the misuse of consumers' legitimate existing accounts (including credit- and debit-card and non-card accounts) increased by 36 percent since 2012. JAVELIN STRATEGY & RESEARCH, 2014 IDENTITY FRAUD REPORT 11 (Feb. 2014). The Report specifically attributed that increase "to the increasing availability of compromised credentials online, in databases gleaned from data breaches and malware." *Id.* The Report also found that existing non-card fraud, involving misuse of loan accounts, Internet accounts such as eBay and Amazon, and online payment accounts such as eBay, had increased nearly threefold since 2012, resulting in losses of $5 billion. *Id.* at 3, 14.

The 2012 Annual Report of the Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center, stated that the 289,874 consumer complaints it received in 2012 had an adjusted dollar loss of $525,441,110. That loss represents an 8.3 percent increase in reported losses since 2011. INTERNET CRIME COMPLAINT CENTER, 2012 ANNUAL REPORT 4 (May 4, 2013), *available at* http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf. A 2013 survey of U.S. and Canadian online merchants found that in 2012, online payments fraud accounted for approximately $3.5 billion in revenue losses. CYBERSOURCE, 2013 ONLINE FRAUD REPORT 4 (2013), *available at* http://form s.cybersource.com/forms/fraudreport2013. In 2013, a number of leading U.S. retail businesses such as Target, Neiman Marcus, White Lodging, Harbor Freight Tools, Easton-Bell Sports, Michaels Stores, and 'Wichcraft reportedly all suffered data breaches of varying sizes stemming from compromise of point-of-sale terminals. *See* MCAFEE, MCAFEE LABS THREATS REPORT: FOURTH QUARTER 2013 5 (2013), *available at* http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2013.pdf.

Businesses may suffer additional adverse effects beyond the immediate loss of funds and customer data. One prominent example of this is Target, which experienced a major data breach in 2013. According to a consulting group, Target reportedly saw its customer traffic in January 2014, both online and in stores, reach its lowest point in 3 years, as 33 percent of U.S. households shopped at Target in January of that year, compared with 43 percent in January 2013. Hadley Malcolm, *Target sees drop in customer visits after breach*, USA TODAY (Mar. 11, 2014), http://www.usatoday.com/story/money/business/2014/03/11/target-customer-traffic/6262059/.

Public and private enterprises in other regions of the world have also come to see cyberfraud as a formidable threat. A recent survey of merchants in the United Kingdom found that in 2012, merchants reported that 1.65 percent of e-commerce revenues were lost to fraud. CYBERSOURCE, THE TURNING

POINT: 2013 UK ECOMMERCE FRAUD REPORT 3 (2013), *available at* http://forms.cybersource.com/forms/ukfraudreport2013. This number, incidentally, is 1.8 times greater than the 0.9 percent of online revenue that U.S. and Canadian enterprises reported were lost to fraud in 2012. CYBERSOURCE, 2013 ONLINE FRAUD REPORT 4 (2013), *available at* http://forms.cybersource.com/forms/fraudreport2013. In March 2014, CIFAS, the United Kingdom's fraud prevention service, reported that 90 percent of identity fraud on plastic payment cards was occurring online. CIFAS, FRAUDSCAPE 9 (2014), *available at* http://www.cifas.org.uk/fraudscape_twentyfourteen.

In Australia, the Australia Institute of Criminology 2012 online survey of Australian consumers found that 95 percent of the respondents had received a scam invitation of some type, with email as the most common method of delivering a fraudulent solicitation (reported by 72 percent of respondents), and that 8 percent of respondents reported having lost money—approximately AU $8,000 per person on average. PENNY JORNA & ALICE HUTCHINGS, AUSTRALIAN INSTITUTE OF CRIMINOLOGY, AUSTRALASIAN CONSUMER FRAUD TASKFORCE: RESULTS OF THE 2012 ONLINE CONSUMER FRAUD SURVEY, TECHNICAL AND BACKGROUND PAPER 56 v, xii, 7–11 (2013), http://www.aic.gov.au/media_library/publications/tbp/tbp056/tbp056.pdf. The survey also noted that the mean loss to scams was AU $7,908, even though the median loss was only AU $500, *see id.* at xii, 11, which appears due to the reporting of other scams in which victims were defrauded of lesser amounts of money, such as the so-called "Microsoft" (computer-repair) scam and work-at-home schemes. *See id.* at 10. And in Oman, in the first quarter of 2013 a leading financial institution reportedly suffered a loss of nearly U.S. $39 million—around 10.5 percent of the bank's estimated 2013 earnings—from a cyberfraud scheme that used prepaid cards to make fraudulent funds transfers. *See* Beatrice Thomas, *Bank Muscat posts $266m profit, despite cyber fraud exposure*, ARABIANBUSINESS.COM (Oct. 28, 2013), http://www.arabianbusiness.com/bank-muscat-posts-266m-profit-despite-cyber-fraud-exposure-524501.html.

II. Extortion- and intimidation-based schemes

Although there are many varieties of fraud schemes that exploit the Internet and computing, one of the most noteworthy cyberfraud trends has been the growth of schemes that go beyond traditional fraud techniques and use extortionate, intimidating, or other fear-inducing language to make victims believe they have no choice but to send the funds that the schemes demand. As shown below in Table 1, there are seven distinguishable types of such schemes, defined in terms of (1) whether the threat is direct or indirect (that is, directed at the victim being contacted or at another person known to the victim), and (2) what type of harm is threatened (that is, whether the scheme threatens physical harm, law enforcement action such as arrest, harm to financial data, or psychological harm).

Table 1: Cyberfraud Schemes Involving Extortionate, Intimidating, or Fear-Inducing Language

Type of Threat	*Direct Threat*	*Indirect Threat*
Physical Harm	Jamaican-Operated Lottery	"Grandparent" - Assault/Accident , Email Address Book
Law Enforcement Action (*e.g.*, Arrest)	Ransomware	"Grandparent" – Arrest, Email Address Book
Harm to Financial Data	Phishing/Malware	"Technical Support"
Psychological Harm	Sexual Blackmail	—

A. Jamaican-operated lottery schemes

The most egregious example of cyberfraud using direct threats of physical harm is the version of fraudulent lottery schemes that Jamaica-based persons conduct. Though largely similar to traditional lottery schemes, which falsely promise victims substantial lottery winnings once they have paid bogus

"fees" or "taxes," Jamaica-based schemes routinely go beyond traditional fraudulent pitches by email or telephone and use express or implied threats of violence to induce victims to make demanded payments. *See* Connie Thompson, *Foreign lottery scams turn violent*, KOMONEWS.COM (Mar. 27, 2013), http://www.komonews.com/news/consumer/Foreign-lottery-scams-turn-violent-200163221.html.

For example, in a 2012 voicemail left for a woman in her seventies, one caller said, "Why you don't want to pick the (expletive) phone up. Pick the (expletive) phone up and stop playing games with me. Want me to come over there and set your home on fire?" CBS News, *Inside the "Jamaican Lottery Scam": How U.S. seniors become targets*, CBS THIS MORNING (Mar. 12, 2013), http://www.cbs news.com/news/inside-the-jamaican-lottery-scam-how-us-seniors-become-targets/. In some cases, callers reportedly used Google Earth to determine the appearance of the victim's home, then gave that description to the victim to make the victim believe that the caller was actually in his or her neighborhood. Associated Press, *Jamaican lottery scams spread despite US crackdown*, FOX NEWS (Apr. 17, 2012), http://www.foxnews.com/world/2012/04/17/jamaican-lottery-scams-spread-despite-us-crackdown/.

B. "Ransomware" schemes

A second major example of extortion-related cyberschemes involving direct threats—a technological refinement of mass-marketing schemes in which criminals purport to be police or federal law enforcement officials—involves the use of so-called "ransomware." Schemes that use a ransomware program place the program on a variety of Web sites, including those that offer pornography or access to illegally downloaded content. When an Internet user visits a site infected with ransomware, the program, without the user's knowledge, downloads to his computer. Shortly thereafter, it manifests itself as a screen that suddenly appears on the user's computer and contains various types of messages intended to make the user believe that he is seeing an official warning message from a law enforcement or government agency. The malware locks the ransomware screen so that the user cannot exit from or delete the screen, and (absent the downloading of antimalware to remove the program) makes it effectively impossible for the user to use the computer in any other way.

The content of the ransomware message varies from country to country, but typically contains language warning the user that he has accessed child pornography or illegally downloaded content and threatening him with arrest or prosecution unless he pays a significant fine, in amounts typically ranging from $100 to several hundred dollars. *See, e.g.*, James Henderson, *Naked sex chats help blackmail Kiwis out of $4.4m*, TECHDAY (Aug. 12, 2013), http://techday.com/netguide/news/naked-sex-chats-help-blackmail-kiwis-out-of-4-4m/168055/. Payment is made via a money-transfer service, such as Green Dot MoneyPak, through which fraudsters can quickly access and withdraw the victim's payment.

Law enforcement authorities have identified examples of ransomware that use the names and official seals of dozens of national law enforcement and government agencies in Australia, Europe, the Middle East, and North and South America. These examples indicate that ransomware schemes are targeting a wide variety of countries around the world, in numerous languages. Moreover, the growth of ransomware variations has been dramatic. McAfee Labs reported that it detected 250,000 unique samples of ransomware in the first quarter of 2013—more than double what McAfee obtained in the first quarter of 2012. Ted Samson, *Update: McAfee: Cyber criminals using Android malware and ransomware the most,* INFOWORLD (June 3, 2013), http://www.infoworld.com/t/security/mcafee-cyber-criminals-using-android-malware-and-ransomware-the-most-219916.

Certain recent examples of ransomware reflect exceptional degrees of ingenuity and callousness in their operation. A relatively new ransomware variant, Kovter, uses information gathered from the victim's browser to make the scam message seem more credible. Lucian Constantin, *Ransomware uses victims' browser histories for increased credibility*, INFOWORLD (Apr. 1, 2013), http://www.infoworld.com/d/security/ransomware-uses-victims-browser-histories-increased-credibility-215560. It will list the

computer's IP address, its host name, the DOJ/DHS/FBI insignias, and a Web site on which the "illegal" material was downloaded. If there is a match between the browser's history and a pornography site, it will display that site. If there is no match, then it will choose a pornography site at random.

Another type of ransomware uses a ransomware screen that displays the name of the German *Bundeskriminalamt* (Federal Police Office), and includes both an accusation of child pornography and images that appear to be actual child pornography embedded in the screen, as well as the name, age, and location of each purported victim and an accusation that those images were viewed on the user's computer. *See* Iain Thomson, *German ransomware threatens with sick kiddie smut*, THE REGISTER (Apr. 5, 2013), http://www.theregister.co.uk/2013/04/05/iwf_warning_smut_ransomware/; *Peel Police warning public about online extortion scam*, 680NEWS.COM (Jan. 22, 2013), http://www.680news.com/2013/01/22/peel-police-warning-public-about-online-extortion-scam/. Yet another variation is the "CryptoLocker" ransomware scheme. Schemes that use CryptoLocker, as a 2013 IC3 public service announcement explained, use

> verbiage in the window [which] states that important files have been encrypted using a unique public key generated for the computer. To decrypt the files you need to obtain the private key. A copy of the private key is located on a remote server that will destroy the key after the specified time shown in the window. The attackers demand a ransom of $300.00 to be paid in order to decrypt the files. Unfortunately, once the encryption of the files is complete, decryption is not feasible. To obtain the file specific Advanced Encryption Standard (AES) key to decrypt a file, you need the private RSA key (an algorithm for public key cryptography) corresponding to the RSA public key generated for the victim's system by the command and control server. However, this key never leaves the command and control server, putting it out of reach of everyone except the attacker.

Internet Crime Complaint Center, *Public Service Announcement: Cryptolocker Ransomeware Encrypts User's Files* (Oct. 28, 2013), http://www.ic3.gov/media/2013/131028.aspx.

There are no reliable estimates of the total number of individuals who have paid ransomware schemes. Researchers at a leading antivirus company, Symantec, estimated that ransomware

> is highly profitable, with as many as 2.9 percent of compromised users paying out. An investigation into one of the smaller players in this scam identified 68,000 compromised computers in just one month, which could have resulted in victims being defrauded of up to $400,000 USD. A larger gang, using malware called Reveton (aka Trojan.Ransomlock.G), was detected attempting to infect 500,000 computers over a period of 18 days.

GAVIN O'GORMAN & GEOFF MCDONALD, RANSOMWARE: A GROWING MENACE 1 (Nov. 2012), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf.

C. Phishing and related malware

A third category of cyberfraud involving direct (though not explicit) threats to victims' financial assets, familiar to many law enforcement and computer-security experts, is the use of "phishing" software and other malware to obtain individuals' financial and personal data. Phishing involves the sending of mass emails to various persons, purportedly from a trustworthy source, such as a bank or law enforcement agency, with messages indicating that the recipient has some imminent threat to his bank account or other personal data that requires immediate attention. In the early versions of phishing, once a recipient was intimidated by the email message into clicking on a link embedded in the email, he or she was presented with a fraudulent popup window or Web site that appears to be associated with a legitimate sender, into

which he or she would be urged to enter significant personal data, such as bank and payment-card data, that is useful for online fraud or identity theft.

More recent variants of phishing rely on infection of Web sites with malicious code that may contain "backdoor" or "keystroking" programs. In these variants, once the email recipient clicks on the embedded link and is taken to the infected Web site, the malware on that site immediately downloads the malicious programs onto the email recipient's computer without his or her knowledge, allowing the phishing scheme's participants to exploit data on victims' computers at later dates.

In February 2014, a leading private-sector coalition dedicated to combating criminal malware of all types, the Anti-Phishing Working Group (APWG), issued a report on phishing trends in the third quarter of 2013. According to the report, overall phishing activity "was up by 20 percent from the previous quarter despite an 8 percent decline in the number of brands targeted." ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS REPORT: 3RD QUARTER 2013 i (Feb. 10, 2014), *available at* http://docs.apwg.org/reports/apwg_trends_report_q3_2013.pdf. The Report also found that "[m]alware creation hit a new record high in the third quarter of 2013," with nearly 10 million new malware samples catalogued. *Id.* at 8.

Although malware writers typically keep their distance from the day-to-day operations of cyberfraud rings, there are circumstances in which creators of cyberfraud-related malware can be identified and apprehended. In January 2014, in *United States v. Panin*, a Russian national pleaded guilty to conspiracy to commit wire and bank fraud for his role as the primary developer and distributor of malicious software known as "SpyEye," which reportedly had infected more than 1.4 million computers in the United States and abroad. SpyEye

> is a sophisticated malicious computer code that is designed to automate the theft of confidential personal and financial information, such as online banking credentials, credit card information, usernames, passwords, PINs, and other personally identifying information. The SpyEye virus facilitates this theft of information by secretly infecting victims' computers, enabling cyber criminals to remotely control the infected computers through command and control (C2) servers. Once a computer is infected and under their control, cyber criminals can remotely access the infected computers, without authorization, and steal victims' personal and financial information through a variety of techniques, including web injects, keystroke loggers, and credit card grabbers. The victims' stolen personal and financial data is then surreptitiously transmitted to the C2 servers, where it is used to steal money from the victims' financial accounts.

Press Release, U.S. Attorney's Office, Northern District of Georgia (Jan. 28, 2014), *available at* http://www.fbi.gov/atlanta/press-releases/2014/cyber-criminal-pleads-guilty-to-developing-and-distributing-notorious-spyeye-malware.

In this case, the defendant was the primary developer and distributor of SpyEye. Operating from Russia from 2009 to 2011, he conspired with others, including a codefendant, an Algerian national, to develop, market, and sell various versions of SpyEye and component parts online. He also

> allowed cyber criminals to customize their purchases to include tailor-made methods of obtaining victims' personal and financial information, as well as marketed versions that targeted information about specific financial institutions including banks and credit card companies. [The defendant] advertised the SpyEye virus on online, invite-only criminal forums. He sold versions of the SpyEye virus for prices ranging from $1,000 to $8,500. [He] is believed to have sold the SpyEye virus to at least 150 "clients," who, in turn, used them to set up their own C2 servers. One of [his] clients, "Soldier," is reported to have made over $3.2 million in a six-month period using the SpyEye virus.

Id.

D. Sexual blackmail

One of the most widely reported and pernicious varieties of cyberfraud involves the targeting of individuals—often teenagers, but also including mature adults—for the purpose of inducing them to undress and expose themselves on Skype, then taking their pictures, and later threatening to post the compromising photographs or video online unless the victim makes extortionate payments. Romance scheme participants use this technique to ensure that their victims comply with demands for money.

The potential for extreme embarrassment reportedly prompts many victims to make the payments. *See* MONICA WHITTY & TOM BUCHANAN, THE PSYCHOLOGY OF THE ONLINE DATING ROMANCE SCAM 5, 10 (Apr. 2012), *available at* http://www2.le.ac.uk/departments/media/people/monica-whitty/Whitty_romance_scam_report.pdf. The financial demands are typically the principal factor that distinguishes these schemes from "catfishing" (that is, "[t]he phenomenon of internet predators that fabricate online identities and entire social circles to trick people into emotional/romantic relationships (over a long period of time)." URBAN DICTIONARY, http://www.urbandictionary.com/define.php?term=Catfishing.

In the United States, in 2011 the Internet Crime Complaint Center (IC3) issued an alert reporting that it had received more than 50 complaints reporting extortion emails that targeted professionals, mainly physicians. The emails told prospective victims that "complaints had been filed against them and posted online, claiming they were facing prison for sexual indecency," together with the victims' names, addresses, telephone numbers, and email addresses. The victims were told that "these types of comments will destroy your reputation and are permanently archived on search engine sites; you will lose thousands of dollars in revenue with a bad reputation." For a fee of $250, the sender promised that he could "convince the people who posted the comments to remove them." Internet Crime Complaint Center, *Internet Crime Complaint Center's (IC3) Scam Alerts* (July 14, 2011), http://www.ic3.gov/media/2011/110714.aspx. In 2013, the IC3 issued another alert about online sexual extortion schemes, stating that it had received numerous complaints over the last couple of years. The IC3 reported at that time that the extortionate demands, which ranged from $50 to $300, sought wiring of the funds to various foreign destinations. Internet Crime Complaint Center, *Internet Crime Complaint Center's (IC3) Scam Alerts* (May 2, 2013), http://www.ic3.gov/media/2013/130502.aspx.

In one 2013 case, an individual was convicted in the Central District of California on charges stemming from his running an extensive online extortion scheme that included hacking. According to the indictment, the defendant hacked into victims' email accounts and changed the passwords, which locked victims out of their online accounts. Once he controlled those accounts, the defendant searched emails or other files for naked or semi-naked pictures of the victims, as well as other information, such as passwords and the names of their friends. Using that information, the defendant posed online as women, sent instant messages to their friends, and persuaded the friends to remove their clothing so that he could view and take pictures of them.

When the victims discovered that they were not speaking with their friends, the defendant "often extorted them again, using the photos he had fraudulently obtained to again coerce the victims to remove their clothing on camera. . . . [He] repeatedly contacted victims to demand that they expose their breasts to him on Skype, and used their email and Facebook accounts to make contact with other victims." He also allegedly posted nude photos of some victims on their Facebook pages when they failed to comply with his demands. At the time of his arrest, authorities estimated that he had victimized more than 350 women, but had not identified all of the victims whose accounts were hacked. Authorities found approximately 3,000 pictures of nude or semi-nude women—some of which were taken from their online accounts, and some of which were taken by the defendant on Skype—on the defendant's computer. Press Release, U.S. Attorney's Office, Central District of California (Jan. 29, 2013), *available at* http://www.justice.gov/usao/cac/Pressroom/2013/016.html. After pleading guilty to felony counts of computer hacking and aggravated identity theft, in December 2013, he was sentenced to 60 months imprisonment. The

sentencing judge characterized him as a "cyber terrorist." Press Release, U.S. Attorney's Office, Central District of California (Dec. 9, 2013), *available at* http://www.fbi.gov/losangeles/press-releases/2013/glendale-man-who-admitted-hacking-into-hundreds-of-computers-in-sextortion-case-sentenced-to-five-years-in-federal-prison.

In another 2013 case, a man who allegedly had been abusing a young female relative took naked photographs and videos of the relative and posted them on the social-networking site Mocospace.com. He then targeted several men, using a fake name and an email address, pretty-gurl985@yahoo.com, to obtain their phone numbers and send them the photos and videos. After the victims received the content, the alleged operator of the scheme then called the victims, pretending to be the girl's outraged father, and demanding "payment of thousands of dollars to cover the cost of her counseling" and threatening to call police and his employers if his demands were not met.

The alleged operator reportedly demanded $5,000 from one of the alleged victims, a Texas A&M University professor. The professor paid $1,000 and promised to pay more, but committed suicide by jumping from a campus parking garage. One of the victim's last acts was reportedly to send a text message to the alleged blackmailer, saying, "Killing myself now. And u will be prosecuted for blackmail." Lee Moran, *Texas A&M professor kills himself after being caught up in blackmail catfish scam*, NEW YORK DAILY NEWS (Mar. 26, 2013), http://www.nydailynews.com/news/crime/blackmailed-professor-kills-scam-article-1.1299173.

Law enforcement authorities in Asia, Australia, Canada, Europe, and New Zealand have reported very similar techniques directed at residents of their regions.

E. "Grandparent schemes" and email address book takeover schemes

Two frequently reported types of cyberfraud schemes involving indirect threats (that is, threats against persons other than the intended victim) are the so-called "grandparent scam" and schemes involving takeover of an email user's email address book. Over the last several years, law enforcement authorities in Australia, Canada, Japan, the United States, and other countries have observed the increasing use of "grandparent" scams. These schemes involve a caller who deceives the person called, often a senior citizen, into believing that the caller is his or her son, daughter, grandson, granddaughter, or other relative.

Because these calls are typically "cold calls," the caller does not use an actual name at the outset, but simply says something like, "Grandma, it's me." The object is to create confusion and uncertainty on the part of the person called. If the call recipient responds with a question, such as "John, is that you?" the caller immediately agrees, then asserts that he is in urgent need of immediate financial assistance.

One form of this scam involves false statements that the caller has been the victim of an assault or an accident and needs money for medical bills. *See, e.g.*, Canadian Anti-Fraud Centre, *Emergency or "Grandparent" Scam* (2008), http://www.antifraudcentre-centreantifraude.ca/english/recognizeit_emergency.html. If the call recipient sends money in response to the first call, a participant in the scheme may call back a second time with another request for money, such as a request for travel funds to return home.

Another form of this scheme involves false statements that the caller has been arrested and needs money for bail or an attorney. In one version of this scam, a U.S. couple was defrauded of $5,400 by a caller who stated that he was with the U.S. Embassy in Madrid and that their grandson had been arrested for speeding and that the police had found marijuana in his car. The caller then put the "grandson" on the phone, and the "grandson" said that he could not talk long and pleaded, "Please don't call mom. She will disown me." Believing that their grandson needed money for his trial and for a flight home, the couple transferred $2,600 through Western Union. They later sent an additional $2,800 when they received a call saying that their grandson had missed his flight and needed more money. Later, when FBI agents interviewed the couple, the couple learned that the calls had apparently come from Canada rather than

Spain. *See* Susan Salisbury, *Scam calls target seniors: 'It's me, Grandma!'*, PALM BEACH POST (Dec. 23, 2010), http://www.palmbeachpost.com/news/business/scam-calls-target-seniors-its-me-grandma/nLnqt/.

Grandparent-scam demands for funds from prospective victims in Australia, Canada, and the United States have ranged from several hundred to several thousand dollars, but have sometimes succeeded in obtaining as much as U.S. $33,000. *See, e.g.*, Western Australia Dep't of Commerce, *Help me scam—also called the "Grandparent" scam*, DEP'T OF COMMERCE (2013), http://www.scamnet.wa.gov.au/scamnet/Types_Of_Scams-Social_networking_scams-Help_me_scams.htm; Melanie Hicken, *'Grandparent scams' steal thousands from seniors*, CNN MONEY (May 22, 2013), http://money.cnn.com/2013/05/22/retirement/grandparent-scams/. In a 2013 incident in Japan, a 73-year-old woman in Saitama received a call from a man who said that he was her nephew, and that he had lost a bag containing a check for ¥30 million (approximately €223,000, £189,000, or U.S. $305,000) from his company. The woman agreed to the caller's request that she could lend him half the amount of the check while his boss's wife covered the other half. She withdrew ¥15 million from a safe deposit box and went to a railway station, where she gave the money to a man "who identified himself as the son of her nephew's boss . . . ." *73-year-old woman conned out of Y15 mil in 'ore-ore' scam*, JAPAN TODAY, (Aug. 2, 2013), http://www.japantoday.com/category/crime/view/73-year-old-woman-conned-out-of-y15-mil-in-ore-ore-scam.

There are few statistics on the current incidence and aggregate losses of grandparent schemes. In the United States, the Federal Trade Commission (FTC) reported that in 2013, it received 121,720 complaints on all types of impostor schemes, including grandparent scams as well as other schemes that involve impersonation of others. *See* U.S. FEDERAL TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY – DECEMBER 2013 at 6 (Feb. 2014), http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf. That represents an increase of nearly 47 percent over the 82,896 impostor-scheme complaints the FTC received in 2012. *See* U.S. FEDERAL TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY—DECEMBER 2012 at 6 (Feb. 2013), http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf. The most detailed national data are for Japan, where the grandparent scam has been active for at least a decade. *See 'It's me, send money' scam creator tells his story in new book*, JapanToday.com (Apr. 27, 2012), http://www.japantoday.com/category/kuchikomi/view/its-me-send-money-scam-creator-tells-his-story-in-new-book.

A second type of cyberfraud scheme that exploits indirect threats to other persons involves hacking an Internet user's email address book, changing the password to the email account so that only the scheme's participants can access it, then sending a blast email to the addressees falsely stating that the sender is abroad and has suffered an accident, a loss of luggage and valuables, a mugging, or even an arrest and urgently needs money. Sometimes called the "stranded traveler" scam, this scheme has targeted individuals in the United States, Canada, New Zealand, and the United Kingdom. *See* Elisabeth Leamy and Sally Hawkins, *'Stranded Traveler' Scam Hacks Victims' Emails, Asks Their Contacts For Money*, ABC NEWS (July 13, 2012), http://abcnews.go.com/Technology/stranded-traveler-scam-hacks-victims-emails-asks-contacts/story?id=16774896.

Two features of this scheme may contribute to its effectiveness. First, the fact that many people who know the true sender simultaneously receive emails from someone whom they perceive to be a credible source can speed the scheme's receipt of funds from multiple sources over a short period of time. Second, because the schemers change the account's password, any efforts by the email recipients to communicate with the purported sender simply enables the schemers to send follow-up emails that purport to confirm the plight of the "sender."

F. "Technical support" schemes

One of the most frequently reported cyberfraud schemes involves call-center operations, typically based in India, that contact people in other countries and falsely represent themselves to be affiliated with

Microsoft. The callers typically use social engineering techniques to persuade the call recipients that their computers have been infected with malicious software and that they need to pay for "technical support" to fix the problem. In some cases, the schemes not only obtain a payment from the victim, but also install malware on the victims' computers so that they can later access victims' financial accounts.

A detailed example of this scheme was documented in 2013 by a senior security researcher at an anti-malware company, who received a "technical support" call. The caller, a woman, first directed him to open Event Viewer, an actual Microsoft tool that displays detailed information about significant events on a computer "that can be helpful when troubleshooting problems and errors with Windows and other programs." *Open Event Viewer*, MICROSOFT.COM, http://windows.microsoft.com/en-us/windows-vista/open-event-viewer. Because Event Viewer displays all Microsoft error reports, the caller asked the researcher

> to count the number of red cross-marked errors and yellow warnings, before warning him: "These errors and warnings are very much harmful for your computer. These are major problems and it doesn't matter if you have one or two errors or more than that. Each one has already started corrupting your whole computer system."

Olivia Solon, *What happens if you play along with a Microsoft 'tech support' scam?*, WIRED, (Apr. 11, 2013), http://www.wired.co.uk/news/archive/2013-04/11/malwarebytes.

After using additional social engineering tricks—such as mischaracterizing the contents of his "Prefetch file" (actually a Windows subfolder that keeps track of the way a computer starts and which programs the user commonly opens) as "100 hacking folders" that placed him "at very high risk"—she turned the call over to a male "technician." The "technician" tried to persuade the researcher that he should register for a lifetime warranty renewal for $299, and opened a browser on his computer through TeamViewer, which gives control of the computer to a third party, so that the researcher could enter his banking information to make the $299 payment through PayPal. When the researcher deliberately entered incorrect banking data, the "technician" retaliated by deleting all of the documents on the researcher's computer, trying to delete the researcher's Ethernet adapter driver, and posting "bye asshole" in the TeamViewer chat log. *Id.*

In addition to the India-based technical support scams that exploit the Microsoft name, there are indications that some India-based schemes are now targeting Apple computer owners. In October 2013, one security researcher discovered an online advertisement for a company called "Speak Support" that purported to offer Mac technical support, claiming that it had an "elite band of tech support experts" and that "Apple Consultants are online." Although the Speak Support Web site represented that it was located in Freehold, New Jersey, domain name registration for two domain names associated with Speak Support traced back to two individuals and contact information in New Delhi, India. When the researcher called the Speak Support toll-free number, the Speak Support representative used social engineering techniques in an effort to persuade the researcher that his computer had error messages and that he needed to pay $200 for technical support. *See* Jerome Segura, *Tech Support Scams: Coming to a Mac near you*, MALWAREBYTES.ORG (Oct. 10, 2013), http://blog.malwarebytes.org/intelligence/2013/10/tech-support-scams-coming-to-a-mac-near-you/.

In November 2013, the IC3 reported that some schemes were calling people who had recently purchased software and offering them a "refund" within three to four months of the purchase, either because the intended victim professed to be dissatisfied with the software or because the caller falsely stated that the company was going out of business. Victims who expressed interest in a refund ultimately would be persuaded to open an account via a wire transfer company to receive their refund, but later discovered that funds were taken from their accounts and wired to India. IC3, *Scam Alerts* (Nov. 25, 2013), http://www.ic3.gov/media/2013/131125.aspx.

III. "Cash-out" schemes

Notwithstanding the prevalence of extortion/intimidation cyberfraud schemes, it is important to note that many schemes do not resort to such extreme measures. One significant type of online scheme that does not use extortion or intimidation is the so-called "cash-out" scheme, which relies on hacking to obtain financial data and withdraw funds from victims' accounts without their knowledge or consent. Law enforcement authorities recognize that many of these schemes are conducted by rings based in Eastern Europe, with confederates in the United States.

Two federal prosecutions within the last year provide cogent examples of how cash-out schemes operate. In May 2013, in *United States v. Mircea*, three Romanian nationals made their initial appearance in the Eastern District of New York after being extradited from Romania, to face charges in an indictment that charged them with participating in a sophisticated multi-million dollar cyberfraud scheme that targeted consumers on U.S.-based Web sites such as eBay.com. The defendants and their coconspirators allegedly

> saturated Internet marketplace websites, such as eBay.com, Cars.com, AutoTrader.com, and CycleTrader.com, with detailed advertisements for cars, motorcycles, boats, and other high-value items generally priced in the $10,000 to $45,000 range. Unbeknownst to the buyers, however, the merchandise did not exist. The so-called sellers corresponded with the victim buyers by email, sending fraudulent certificates of title and other information designed to lure the victims into parting with their money. Sometimes, they pretended to sell cars from nonexistent auto dealerships in the United States and even created phony websites for these fictitious dealerships.

Press Release, U.S. Attorney's Office, Eastern District of New York (May 2, 2013), *available at* http://www.justice.gov/usao/nye/pr/2013/2013may02b.html.

After the purported sellers allegedly reached an agreement with the victim buyers, they would often email the buyers invoices, purporting to be from Amazon Payments, PayPal, or other online payment services, with wire-transfer instructions. These invoices, however, were also fraudulent, as the conspirators used counterfeit service marks in designing the invoices so that they would look exactly like communications from legitimate payment services. These invoices directed the buyers to send money to U.S. bank accounts that foreign nationals in the United States, known as "arrows," had opened. The arrows would then collect the fraudulent proceeds and send them to the defendants in Europe by wire transfer and other methods, such as hiding $18,000 worth of cash inside hollowed-out audio speakers. *Id.*

In March 2014, in *United States v. Sharapka*, a federal grand jury in the District of New Jersey returned an indictment against three individuals—two residents of the Ukraine and a resident of Brooklyn—for their roles in an international scheme to use information hacked from customer accounts at more than a dozen banks, brokerage firms, payroll-processing companies, and government agencies, in an attempt to steal at least $15 million from U.S. customers. According to the indictment, after conspiring hackers gained unauthorized access to the bank accounts of customers of more than a dozen global financial institutions, businesses, and government agencies,

> the defendants and conspirators diverted money from them to bank accounts and pre-paid debit cards the defendants controlled. They then implemented a sophisticated "cash out" operation, employing crews of individuals known as "cashers" to withdraw the stolen funds, among other ways, by making ATM withdrawals and fraudulent purchases in New York, Massachusetts, Illinois, Georgia and elsewhere.
>
> As part of the scheme, the defendants stole identities from individuals in the United States, which they used to facilitate the cash out operation, including by

> transferring money to cards in the names of those stolen identities. They also used some of those identities to file fraudulent tax returns with the IRS seeking refunds.

Press Release, U.S. Attorney's Office, District of New Jersey (Mar. 17, 2014), *available at* http://www.justice.gov/usao/nj/Press/files/Sharapka,%20Oleksiy%20et%20al.%20Indictment%20News%20Release.html.

IV. Other cyberfraud schemes

Other cyberfraud schemes rely more heavily on traditional fraud techniques to persuade victims to send or transfer money. Like cash-out schemes, these schemes may be based abroad, but use coconspirators in the United States to facilitate various aspects of the scheme.

One frequently reported type of cyberfraud scheme using traditional techniques involves falsely posting listings of vehicles for sale on online platforms, persuading interested buyers to wire-transfer payments to a financial institution or third party, and then failing to deliver the vehicles and keep the payments. For example, in August 2013, in *United States v. De La Cruz Piote*, a federal grand jury in the Western District of Washington indicted a Spanish national for his role in a scheme to defraud prospective purchasers of cars, boats, and recreational vehicles (RVs) by using false Internet postings and bogus payment-processing programs. According to records filed in the case, the defendant and other coschemers opened multiple bank accounts using various foreign passports and identities. The conspirators set up the accounts with various business names and advertised luxury cars, boats, and RVs on legitimate Web sites, such as Craigslist or Autotrader.com. Using false names, the conspirators would then correspond with potential purchasers to wire funds to one of the business bank accounts, claiming that it was an "escrow account" that would hold the funds until the buyer received the vehicle. To enhance the appearance of legitimacy, the conspirators allegedly would create counterfeit PayPal paperwork and Web pages, or would have the victims make the payment through a service that the conspirators created and called "Amazon Payments," though it was in fact not associated with Amazon.com. Press Release, U.S. Attorney's Office, Western District of Washington (Aug. 15, 2013), *available at* http://www.justice.gov/usao/waw/press/2013/August/piote.html.

In February 2014, a Romanian national pleaded guilty in the Middle District of Tennessee to conspiracy to commit bank and wire fraud for his role in moving approximately $320,000 in illicit proceeds derived from an international online marketplace fraud scheme. According to testimony at the plea hearing,

> members of the conspiracy fraudulently listed vehicles for sale at online marketplaces such as Autotrader and eBay. When potential buyers expressed interest in purchasing the vehicles, co-conspirators sent e-mails that directed the buyers to wire payments to certain bank accounts. In total, 17 individuals sent approximately $321,389 to accounts opened by [the defendant]. None of the victims ever received the vehicles for which they paid
> . . . .
> According to testimony, beginning at least as early as December 2011 and continuing to as late as July 2013, [the defendant] opened bank accounts under false identities, which were supported by fraudulent identity documents including counterfeit passports. [He] opened 10 such accounts, under nine different names [and] subsequently sent the bulk of the money to other co-conspirators located abroad.

Press Release, U.S. Attorney's Office, Middle District of Tennessee (Feb. 7, 2014), *available at* http://www.justice.gov/usao/tnm/pressReleases/2014/2-7-14.html.

V. Prosecution approaches to cyberfraud

Regardless of the technical sophistication that certain cyberfraud schemes employ, or the potential challenges of acquiring digital evidence from multiple jurisdictions, it is important to recognize that cyberfraud, however complex its technological aspects may be, is simple in concept. As cases such as *Mircea*, *Sharapka*, and *Panin* make clear, various general fraud and money-laundering offenses used in other types of fraud cases are entirely suitable to charge members of cyberfraud schemes.

Wire fraud (18 U.S.C. § 1343) is readily applicable to interstate or foreign emails, Web site postings, or accessing of databases in furtherance of a fraud scheme. *See, e.g.*, *United States v. Barrington*, 648 F.3d 1178, 1179 (11th Cir. 2011) (unauthorized accessing of university computers and emailing of keylogged usernames and passwords); *United States v. Carlson*, 209 F. App'x 181, 182 (3d Cir. 2006) (unpublished decision) (spamming of emails from spoofed accounts). Because cyberfraud proceeds are routinely transmitted domestically and internationally, either or both of the principal money-laundering offenses (18 U.S.C. §§ 1956 and 1957)—for which the list of specified unlawful activities includes mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), bank fraud (18 U.S.C. § 1344), access-device fraud (18 U.S.C. § 1029), identification-document fraud and identity theft (18 U.S.C. § 1028), and computer fraud and abuse (18 U.S.C. § 1030), *see* 18 U.S.C. § 1956(c)(7)(A), (D)—are often applicable.

A number of specific fraud offenses and identity-theft offenses may also be appropriate to charge in cyberfraud cases. The access-device section (18 U.S.C. § 1029) includes at least six felonies that may apply to various aspects of cyberfraud schemes: (1) subsection 1029(a)(1) (knowingly and with intent to defraud producing, using, or trafficking in one or more counterfeit access devices), (2) subsection 1029(a)(2) (knowingly and with intent to defraud trafficking in or using one or more unauthorized access devices during any one-year period, and by such conduct obtaining anything of value aggregating $1,000 or more during that period, (3) subsection 1029(a)(3) (knowingly and with intent to defraud possessing fifteen or more devices which are counterfeit or unauthorized access devices), (4) subsection 1029(a)(5) (knowingly and with intent to defraud effecting transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any one-year period the aggregate value of which is equal to or greater than $1,000), (5) subsection 1029(a)(6) (without the authorization of the issuer of the access device, knowingly and with fraudulent intent soliciting a person for the purpose of (A) offering an access device or (B) selling information regarding or an application to obtain an access device), and (6) subsection 1029(a)(10) (without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causing or arranging for another person to present to the member or its agent, for payment, one or more evidences or records of transactions made by an access device).

Moreover, given the breadth of the definitions of terms in § 1029, a cyberfraud defendant may violate one or more of the § 1029 offenses listed above whether or not he ever comes in contact with physical payment or identification cards. Section 1029(e)(1) defines "access device" to mean

> any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

18 U.S.C. § 1029(e)(1) (2014).

In addition, § 1029(e)(2) defines the term "counterfeit access device" to mean "any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device" (18 U.S.C. § 1029(e)(2)), and § 1029(e)(3) defines the term "unauthorized

access device" to mean "any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud." *See* 18 U.S.C. § 1029(e)(3) (2014). Thus, a cyberfraud ring member who participates in unauthorized acquisition, possession, sale, or other transfer of stolen, fraudulently obtained, or hacked identifying or financial data may be violating one or more of the § 1029 offenses.

Because cyberfraud schemes inevitably deal in fraudulently obtained or hacked identifying data, the identity-theft offenses (18 U.S.C. §§ 1028(a)(7) and 1028A(a)) also may apply to members of the scheme. Section 1028(a)(7) prohibits knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law, when the transfer, possession, or use prohibited by this subsection is in or affects interstate or foreign commerce, including the transfer of a document by electronic means. 18 U.S.C. § 1028(a)(7), (c)(3)(A) (2014). A violation of this subsection has a maximum 15-year term of imprisonment if, as a result of the offense, any individual committing the offense obtains anything of value aggregating $1,000 or more during any one-year period. 18 U.S.C. § 1028(b)(1)(D) (2014).

Section 1028A(a), the aggravated identity theft offense, has a number of elements in common with § 1028(a)(7), although neither is a lesser included offense of the other. It prohibits, during and in relation to any of the felony violations enumerated in § 1028A(c), knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person, when the defendant knows that the means of identification in question belongs to another real person. *See* 18 U.S.C. § 1028A(a) (2014); *Flores-Figueroa v. United States*, 129 S. Ct. 1886, 1894 (2009). Conviction of a § 1028A(a) offense carries a fixed two-year term of imprisonment. With limited exceptions, no term of imprisonment imposed on a person under § 1028A "shall run concurrently with any other term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony during which the means of identification was transferred, possessed, or used." 18 U.S.C. § 1028A(b)(2) (2014).

It should be noted that the term "means of identification" used in both § 1028(a)(7) and § 1028A(a) is defined to include not only standard identifying data, such as name, Social Security number, driver's license number, and passport number, but "access devices" as defined in 18 U.S.C. § 1029, unique biometric data, and even telecommunication identifying information. *See* 18 U.S.C. § 1028(d)(7) (2014). As a result, both identity-theft offenses can reach a wider range of valuable personal data than the access-devices offenses.

In addition to the possible use of other computer-related offenses (for example, 18 U.S.C. § 1030(a)(2)(A)–(C) (unauthorized access) and § 1030(a)(5) (computer damage)), there may be cases in which the computer fraud offense (18 U.S.C. § 1030(a)(4)) would apply to certain participants in cyberfraud schemes. Section 1030(a)(4) prohibits knowingly and with fraudulent intent, "access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period." 18 U.S.C. § 1030(a)(4) (2014). Conviction of a § 1030(a)(4) offense carries a maximum five- or ten-year term of imprisonment, depending on individual facts (18 U.S.C. § 1030(c)(3)(A)–(B) (2014)). Merely hacking into and searching a database for personal data that could be used in a cyberfraud scheme, without more, would not appear to constitute a § 1030(a)(4) violation. *See United States v. Czubinski*, 106 F.3d 1069, 1078–79 (3d Cir. 1997). On the other hand, removing valuable personal data for resale or use in fraudulent transactions would. *See, e.g.*, *United States v. Rake*, No. 01-13921, 2002 WL 34376595 (11th Cir. 2002) (per curiam) (unreported decision).

After conviction in a cyberfraud case, prosecutors should peruse the U.S. Sentencing Guidelines with care to identify all potentially applicable enhancements, such as the following enhancements in U.S.S.G. § 2B1.1:

- Loss: For a count of conviction that involved counterfeit or unauthorized access devices, the $500 per access device threshold. *See* U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 n.3(F)(i).
- Multiple victims: For a count that involves 10 or more victims, the mass-marketing/multiple victim enhancement, which ranges from a 2- to a 6-level increase. *See id.* § 2B1.1(b)(2) n.4(A)–(B), (E).
- Email harvesting: For a count under the CAN-SPAM Act (18 U.S.C. § 1037) that involved obtaining email addresses through improper means, the 2-level § 1037 enhancement. *Id.* § 2B1.1(b)(3).
- Government impostor: For a count that involved a misrepresentation that the defendant was acting on behalf of a government agency, the 2-level "impostor" enhancement. *Id.* § 2B1.1(b)(9).
- Extraterritorial operation/sophisticated means: For a case in which a substantial part of the fraudulent scheme was committed from outside the United States or the offense otherwise involved sophisticated means, the 2-level extraterritorial operation/sophisticated means enhancement. *Id.* § 2B1.1(b)(10)(B)–(C) n.9.
- Access devices: For a count that involved the production or trafficking of any unauthorized or counterfeit access device, the 2-level access-device/authentication feature enhancement. *Id.* § 2B1.1(b)(11)(B) n.10.
- Section 1030/personal information: For a count under 18 U.S.C. § 1030 that involved an intent to obtain personal information or the unauthorized public dissemination of personal information, the 2-level § 1030 enhancement. *Id.* § 2B1.1(b)(17).
- Section 1030/critical infrastructure: For a count that involved certain specified § 1030 offenses affecting critical infrastructure, the § 1030 enhancement that ranges from a 2- to a 6-level increase, depending on the facts. *Id.* § 2B1.1(b)(18) n.14.

VI. Resources for cyberfraud prosecutions

Federal prosecutors handling any cyberfraud investigation, regardless of how simple or complex it seems, should identify and take full advantage of all resources that can assist them in their investigation. For expertise in cybercrime legal and policy issues, of course, the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and the Computer Hacking and Intellectual Property Coordinators in U.S. Attorney's offices and various litigating components of the Department of Justice can be indispensable. But prosecutors should also draw on information resources that can lead to the discovery of cyberfraud victims and additional investigative leads.

The Federal Trade Commission's (FTC's) Consumer Sentinel Network, to cite one example, contains more than 9 million complaints about all types of consumer fraud and identity theft, including Internet-related fraud schemes. Of the more than 2.1 million complaints that the FTC received in 2013, nearly half (48 percent) of those who were contacted by the scheme reported that email or other Internet-related contact (for example, Web sites) were the method of contact (FEDERAL TRADE COMM'N, CONSUMER SENTINEL NETWORK DATABOOK at 3, 9 (Feb. 2014), *available at* http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf. Agents and prosecutors whose offices do not have remote online access to Sentinel can arrange with

the FTC to obtain such access or seek assistance from the FTC staff in identifying and analyzing Sentinel complaint data.

The IC3 also has a substantial repository of cyberfraud complaints from persons in the United States and other countries. In addition to providing a conduit to receive Internet-related complaints, the IC3 staff conducts research related to those complaints and develops analytical reports that are referred to state, local, federal, tribal, or international law enforcement and/or regulatory agencies. Those agencies can then develop investigations based on the forwarded information, as appropriate. *See* INTERNET CRIME COMPLAINT CENTER, 2012 ANNUAL REPORT 4 (May 4, 2013), *available at* http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf. The IC3 also issues, at frequent intervals, public advisories about recent cybercrime trends and techniques, including cyberfraud. *See* PRESS ROOM, http://www.ic3.gov/media/default.aspx.

Finally, when prosecutors handling cyberfraud cases determine that they need to obtain leads, evidence, or cooperation from foreign countries, they should consider not only formal legal mechanisms such as Mutual Legal Assistance Treaties, but mechanisms to secure informal law enforcement assistance. Those include the FBI's Legal Attachés and overseas offices of other federal law enforcement agencies such as the U.S. Secret Service and Homeland Security Investigations. Advice and guidance from these overseas representatives can often save considerable time in determining how best to seek and obtain critical information and assistance for an investigation. In certain cases, entities like CCIPS, the Fraud Section, and specialized multilateral working groups, such as the International Mass-Marketing Fraud Working Group (co-chaired by the Department of Justice), can further assist in identifying foreign law enforcement agencies and contacts with the necessary expertise and authority.

As the World Wide Web reaches its 25th anniversary this month, federal law enforcement can safely assume that criminals will continue to seek out and to exploit rapidly any vulnerabilities, high-tech or low-tech, that enable them to conduct lucrative cyberfraud schemes. The challenge for law enforcement, then, is to become more adept at quickly identifying new vulnerabilities and working with the private and public sectors to eliminate or minimize them before cyberfraud rings can exploit them, and to use the best available technological and legal resources to ferret out such schemes wherever they can be found.❖

ABOUT THE AUTHOR

❑**Jonathan J. Rusch** is Deputy Chief for Strategy and Policy in the Fraud Section of the Criminal Division. His responsibilities include co-chairing the International Mass-Marketing Fraud Working Group and chairing the interagency Bank Fraud Working Group, Identity Theft Enforcement Interagency Working Group, and Mass-Marketing 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 Trial Advocacy, and Lecturer in Law at the University of Virginia Law School, where he teaches Cybercrime. He has written law review articles on various aspects of cybercrime-related law. He also will teach a course on Global Cybercrime Law at the China University of Political Science and Law in Beijing. ✠

Cybersecurity: The Urgent Challenge of Our Time

Sean B. Hoar
Assistant United States Attorney
District of Oregon

Brian Krebs, *Hacker Ring Stole 160 Million Credit Cards*, KREBSONSECURITY (July 25, 2013), http://krebsonsecurity.com/2013/07/hacker-ring-stole-160-million-credit-cards/; Tech News, *Big Data Breach: 360 Million Newly Stolen Credentials For Sale*, NBCNEWS (Feb. 25, 2014), http://www.nbcnews.com/#/tech/tech-news/big-data-breach-360-million-newly-stolen-credentials-sale-n38741; Kelly Clay, *Forty Million Target Customers Affected by Data Breach*, FORBES (Dec. 18, 2013, 5:57 PM), http://www.forbes.com/sites/kellyclay/2013/12/18/millions-of-target-customers-likely-affected-by-data-breach/; Jia Lynn Yang & Amrita Jayakumar, *Target Says Up To 70 Million More Customers Were Hit by December Data Breach*, THE WASHINGTON POST (Jan. 10, 2014), http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html; Damon Poeter, *Adobe Hacked, Data for Millions of Customers Stolen*, PC (Oct. 3, 2013), http://www.pcmag.com/article2/0,2817,2425215,00.asp; Angela Moscaritolo, *1.1 Million Cards Compromised in Neiman Marcus Hack*, PC (Jan. 24, 2014), http://www.pcmag.com/article2/0,2817,2429872,00.asp; Abigail Wang, *Data Breaches Hit All Time High In 2013*, PC (Jan. 31, 2014), http://securitywatch.pcmag.com/security/320072-data-breaches-hit-all-time-high-in-2013.

On an almost daily basis, we are reminded of the vulnerability of our digital infrastructure. Securing our digital infrastructure is one of the most important challenges of our time. It controls and supports our critical infrastructure, which is essential to life as we know it. Viewed from a national perspective, our critical infrastructure is comprised of 16 "sectors": chemical, commercial facilities, communications, critical manufacturing, dams, defense, emergency services, energy, financial services, food and agriculture, government facilities, healthcare, information technology, nuclear, transportation, and water. Our digital infrastructure is the nervous system, the control system, for each of these sectors—from electrical grids to stock markets. A secure digital infrastructure is essential to our economy, our public health, and our national security.

As federal prosecutors, we probably have a heightened sense of the dangers that lurk in our digital environment—beginning with the "dark side" of the Internet. Those of us who are part of the national network coordinated by the Computer Hacking and Intellectual Property Section (CCIPS) (designated as Computer Hacking and Intellectual Property (CHIP) Coordinators, or lead cyber attorneys) witness on a regular basis the damage caused by system intrusions and other malicious online exploits. CHIP Coordinators, or lead cyber attorneys, are responsible for conducting outreach and educating others in both the public and private sector about cybercrime-related issues. Consistent with that responsibility, this article provides background on recent developments and standards for securing our digital infrastructure, perhaps the most important issue of our time.

This article addresses two internationally recognized sets of network security protocols in an attempt to outline "talking points" for outreach to the public and private sector. The "talking points" barely touch the surface of network security, but serve as an outline for best practices. The article also references several regulatory schemes concerned with information privacy and data protection. These schemes serve as an important reminder about the sectors of information vulnerable to exploitation in an insecure digital infrastructure. The bottom line is that systems containing data that can be stolen and

monetized are continuously being attacked. It is not enough to be "compliant" with the various regulatory schemes. Information technology systems must be proactively robust, and continuously monitoring and improving their security perimeter.

Several of the federal regulatory schemes that may give rise to litigation and/or enforcement action in the event of a data breach and information compromise are:

1. Children's Online Privacy Protection Act requires covered Web site operators to maintain reasonable procedures to protect the personal information of children under the age of 13.
2. Communications Act, § 222, requires protection of communication subscriber information.
3. Electronic Communications Privacy Act requires protection of stored electronic communications.
4. Fair Credit Reporting Act imposes requirements for the collection, disclosure, and disposal of data collected by consumer reporting agencies.
5. Federal Trade Commission Act, § 5, is an enforcement mechanism against unfair and deceptive business practices, which may result through data breach or information compromise.
6. Gramm-Leach-Bliley Act requires "financial institutions" (broadly defined to include banks, mortgage companies, insurance companies, financial advisors, investment firms, etc.) to protect certain account holder information.
7. Health Insurance Portability and Accountability Act requires covered entities (healthcare providers, health plans, healthcare clearinghouses) to maintain security standards for protected health information.
8. Health Information Technology for Economic and Clinical Health Act strengthens penalties for HIPAA violations and extends HIPAA violation liability to "business associates" to whom protected health information is disclosed.
9. Payment Card Industry Data Security Standard requires merchants accepting payment cards to safeguard cardholder data.

Also, 46 states have data breach disclosure laws; only Alabama, Kentucky, New Mexico, and South Dakota do not. Internationally, the European Union Privacy Directive and the Canadian Personal Information Protection and Electronic Documents Act are comprehensive national programs which protect the processing of personal information.

I. Executive Order 13636, Improving Critical Infrastructure Cybersecurity

On February 12, 2013, President Obama issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity. This Executive Order reflected the recognition that a secure digital infrastructure is critical to the economic and national security of the United States. The Executive Order directed the National Institute of Standards and Technology (NIST) to work with public and private sector stakeholders to develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cyber risks to critical infrastructure. One year later, on February 12, 2014, NIST released the first version of the Framework for Improving Critical Infrastructure Cybersecurity. The Framework is a risk management tool to assist organizations in assessing cybersecurity risks, protecting against attacks, and detecting intrusions as they occur. The Framework uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs, without imposing additional regulatory burdens.

II. Framework for Improving Critical Infrastructure Cybersecurity

The Framework applies to organizations that comprise critical infrastructure. Even non-critical infrastructure organizations, however, should assess whether their own risk management practices meet the Framework standard. Although compliance with the Framework is voluntary, all organizations should consider implementing it on an appropriate scale. The pervasive and persistent cybersecurity threat, and the heightened risk of data breach litigation and regulatory action, require deployment of the best available practices. The Framework provides guidance to accomplish this outcome.

The Framework is intended to complement, not replace, existing organizational processes and cybersecurity protocols. Organizations can utilize the Framework to enhance their management of cybersecurity risk while aligning with industry best practices. An organization without an existing cybersecurity program can use the Framework as a reference to establish one.

The Framework is technology neutral, which ensures extensibility and enables technological innovation. It relies on a variety of existing global standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience. These standards, guidelines, and practices have been developed, managed, and updated by industry and allow geographic and technological scalability. Building upon this foundation, the Framework provides a common taxonomy and mechanism for organizations to do the following:

1. Describe their current cybersecurity posture
2. Describe their target state for cybersecurity
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
4. Assess progress toward the target state
5. Communicate among internal and external stakeholders about cybersecurity risk

The Framework is neither industry nor country specific. Organizations throughout the world can use the Framework to enhance their own cybersecurity efforts. The common taxonomy of standards, guidelines, and practices contribute to the development of a common language for international cooperation on critical infrastructure cybersecurity.

The Framework consists of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profile. The Framework Core is a set of cybersecurity activities, desired outcomes, and informative references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across organizations from the executive to the operations level. The Framework Core consists of five concurrent and continuous functions:

1. Identify: develop organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
2. Protect: develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
3. Detect: develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
4. Respond: develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
5. Recover: develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

When considered together, these functions provide a strategic view of the lifecycle of the organizational management of cybersecurity risk. The Framework Core then identifies underlying key categories and subcategories for each function and matches them with informative references such as existing standards, guidelines, and practices, for each subcategory.

The Framework Implementation Tiers provide context on organizational cybersecurity risk and existing processes to manage the risk. The Tiers describe the degree to which organizational risk management practices exhibit desired characteristics defined in the Framework. They reflect a progression from informal, reactive responses to agile and risk-informed approaches. The Tiers provide an organizational risk management selection process, drawing from threat environments, legal and regulatory requirements, business/mission objectives, and organizational constraints.

The Framework Profile represents selected organizational outcomes based on business needs that an organization has selected from the Framework categories and subcategories. It can be characterized as the alignment of standards, guidelines, and practices to particular desired outcomes. A comparative Profile can be used to identify the need for improving cybersecurity, such as a "Current" Profile versus a "Target" Profile. The distance between the two can be used to measure progress when conducting self-assessments.

The following steps illustrate how an organization can use the Framework to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity:

1. Priorities and scope: Identify business/mission objectives and organizational priorities. Make strategic decisions regarding implementation of a cybersecurity program, and determine the scope of systems and assets that support selected business lines or processes. The Framework can be adapted to support different business lines or processes within an organization, which may have different business needs and risk tolerances.
2. Orient: Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and an overall risk approach. The organization then identifies threats to, and vulnerabilities of those systems and assets.
3. Create a current profile: The organization creates a Target Profile that focuses on the assessment of the Framework categories and subcategories describing the organization's desired cybersecurity outcomes.
4. Conduct a risk assessment: The assessment should be guided by the organization's overall risk management process or previous risk assessment activities. An analysis of the operational environment should be done to discern the likelihood of a cybersecurity event and the impact such an event could have on the organization.
5. Create a target profile: The organization creates a Target Profile that focuses on the assessment of the Framework categories and subcategories, describing the organization's desired cybersecurity outcomes.
6. Determine, analyze, and prioritize gaps: The organization compares the Current Profile and the Target Profile to determine gaps. It then creates a prioritized action plan to address gaps and identify resources necessary to address the gaps.
7. Implement action plan: The organization determines which actions to take to address the gaps. It then monitors its current cybersecurity practices to determine whether it aligns with the Target Profile.

The NIST Framework is about risk management, which is the ongoing process of identifying, assessing, and responding to risk. In order to adequately manage risk, organizations must have the capacity to understand the likelihood of a cybersecurity event and the measurable consequences of such an event. In assessing the risk of a cybersecurity event, organizations can determine the allocation of resources to mitigate, transfer, avoid, or accept the risk, all of which may have dramatically different outcomes on the delivery of organizational services. The key is for an organization to use risk management processes to inform, which will assist in allocating resources toward desired outcomes.

The announcement of the NIST Framework was immediately embraced by the Department of Defense (DOD). On March 12, 2014, the DOD Chief Information Officer issued an instruction for DOD to transition from the DOD Information Assurance Certification and Accreditation Process, commonly known by the acronym DIACAP, to NIST's risk management Framework. This Framework was outlined in Special Publication 800-37 and places greater emphasis than DIACAP on standards for continuous monitoring, risk assessment, risk management, and systems' assessment and authorization. In addition to adopting the NIST risk management Framework, DOD mandated that DOD components adhere to the principals established in SP 800-53, NIST's guidance on security and privacy controls for federal information systems, and meet the requirements of the Federal Information Security Management Act, the law that governs federal government information technology security. DOD's adoption of the NIST risk management Framework should improve the ability of the Federal Government to develop better cybersecurity. It will help standardize risk management practices throughout government information technology systems in civilian, defense, and intelligence agencies, resulting in numerous efficiencies and scalable approaches to cybersecurity challenges.

III. SANS 20 Critical Security Controls

The SANS Institute Critical Security Controls are comprised of a prioritized list of network actions involving architectures, processes, products, and services that have proven to be effective against the latest digital threats. The Security Controls focus primarily on prioritizing security functions effective against the latest threats, and also on gaining operational efficiencies and effectiveness through standardization and automation. The actions defined by the Security Controls are essentially a subset of the comprehensive catalog defined by NIST SP 800-53. As such, they do not attempt to replace the work of NIST, including the Framework for Improving Critical Infrastructure Cybersecurity described above. Instead, the Security Controls prioritize a smaller number of actionable controls, which will likely have the most significant impact in securing networks. The following is a list of the Security Controls:

1. Inventory of authorized and unauthorized devices: Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
2. Inventory of authorized and unauthorized software: Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
3. Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers: Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
4. Continuous vulnerability assessment and remediation: Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

5. Malware defenses: Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.
6. Application software security: Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.
7. Wireless access control: Identify and implement processes and tools to track/control/prevent/correct the secure use of wireless local area networks (LANS), access points, and wireless client systems.
8. Data recovery capability: Identify and implement processes and tools to properly back up critical information with a proven methodology for timely recovery of it.
9. Security skills assessment and appropriate training to fill gaps: For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise. Develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.
10. Secure configurations for network devices such as firewalls, routers, and switches: Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change the control process in order to prevent attackers from exploiting vulnerable services and settings.
11. Limitation and control of network ports, protocols, and services: Manage (track, control, correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.
12. Controlled use of administrative privileges: Identify and implement processes and tools to track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
13. Boundary defense: Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.
14. Maintenance, monitoring, and analysis of audit logs: Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.
15. Controlled access based on the need to know: Identify and implement processes and tools to track, control, prevent, and correct secure access to critical assets (for example, information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.
16. Account monitoring and control: Actively manage the life-cycle of system and application accounts—their creation, use, dormancy, deletion—in order to minimize opportunities for attackers to leverage them.
17. Data protection: Identify and implement processes and tools to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.
18. Incident response and management: Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (for example, plans, defined roles, training, communications, management oversight) for quickly

discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

19. Secure network engineering: Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations, while denying or minimizing opportunities for attackers.

20. Penetration tests and red team exercises: Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Each Security Control is accompanied with instructions on how to implement the control (often 10 steps or more), procedures and tools to utilize in implementing the control, questions organizations can address to obtain metrics about the effectiveness of the control, and a diagram depicting how the control can be deployed. These instructions provide information technology personnel step-by-step guidelines and considerations in the application of the respective control so that each one is appropriately extensible and scalable.

IV. Conclusion

Securing our digital infrastructure is one of the most important challenges of our time. It is essential to our economy, our public health, and our national security. Whether organizations follow the NIST Framework, the SANS Institute Security Controls, both, or something in between, it is critical that they create, maintain, and continuously enhance their cybersecurity programs. Our computer networks are under constant attack and cybersecurity is more important than ever before. It is not enough to be "compliant" with the various regulatory schemes. Information technology systems must be proactive and robust, or offensively defensive, in order to meet incredibly challenging demands. The headlines in the first paragraph were simply a snapshot of historical trends, but they reflect a window into our future. We can change that future if we invest in creating a more secure digital infrastructure today—the most urgent challenge of our time. ❖

ABOUT THE AUTHOR

❑ **Sean B. Hoar** has served with the Department of Justice as an Assistant U.S. Attorney since 1991 and is the lead cyber attorney for the District of Oregon. His caseload consists primarily of complex white collar and high-tech crime. He is a Certified Information Privacy Professional/United States (CIPP/US), and teaches courses in cybercrime at the Lewis & Clark Law School and the University of Oregon School of Law. Mr. Hoar also serves as the Executive Director of the Financial Crimes & Digital Evidence Foundation, a non-profit corporation dedicated to training law enforcement officers and their private sector counterparts. ✠

International Cooperation: A Primer of the Tools and Resources Available When Your Investigation Takes You Overseas

Michael Chu
Assistant United States Attorney
Southern District of Texas

As the world becomes a smaller, more connected place, prosecuting cybercrimes increasingly requires cooperation from other countries. But prosecutors sometimes hesitate to get evidence in a foreign country or arrest a fugitive overseas because they are not sure what resources are available. Here are some tools that can help.

I. Preserving evidence

Immediately preserving electronic evidence is the first step in any cybercrime investigation. Even more than physical evidence, electronic evidence is susceptible to disappearing quickly. Sometimes it is because a criminal intentionally hides his tracks by deleting data with a keystroke. Other times, it is simply because of routine business retention practices that allow logs to be systematically overwritten.

These challenges are compounded by the ease by which criminals can insert buffers to further insulate themselves from discovery. For example, criminals can hide their true locations by routing their crimes through proxy computers located in other countries, perhaps by using malware to subvert these computers into participating in the intrusion without their owners' knowledge. Ideally, you could obtain forensic images of those computers, analyze the malware, and try to find the place from where those instructions were being sent.

The bottom line is that the evidence you really want is often several links down the chain. These problems are formidable enough when the evidence is located within the United States—but increasingly, this evidence is located outside our borders.

II. The 24/7 High Tech Crime Network

For urgent assistance in foreign countries, a great resource that is available 24 hours a day, 7 days a week, is the 24/7 High Tech Crime Network. Technically called the "G-8 24/7 High Tech Crime Network," it is actually comprised of far more than just the G-8 countries. Currently, 65 countries worldwide are members.

Members of the 24/7 Network commit to having English-speaking, technologically-proficient points of contact who can help the requesting country preserve electronic evidence held by service providers. These points of contact are also knowledgeable about domestic laws and policies as to both what their laws allow in terms of preservation and seizure of evidence, and what their laws allow them to do for other countries.

They can also alert you if the evidence appears to lead to a third country and, hopefully, provide enough data so you can request assistance from that third country. Perhaps most importantly, they may be

well-situated to opine whether the service provider is law enforcement friendly and will honor legal process or whether it will notify a target.

The 24/7 Network point of contact for the United States is the Computer Crime and Intellectual Property Section (CCIPS) of Main Justice. In addition to the 24/7 Network, CCIPS also has other foreign contacts that might help your case. If your investigation takes you overseas, call 202-514-1026 during business hours (or 202-514-5000 for after hour requests) and ask for the CCIPS duty attorney.

III. The Office of International Affairs, DOJ Attachés, and Law Enforcement Country Attachés

A. Informal or formal assistance: the Office of International Affairs at Main Justice can help determine which is available

Once your evidence is preserved, your first step to obtain that evidence (or to arrest a fugitive located abroad) should be to contact the Office of International Affairs (OIA) at Main Justice. This requirement is enshrined in the U.S. Attorneys' Manual. *See* DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-13.500 to 9-13.900 (2012). However, even if it were not, it would make good sense. Every country is different, and the state of our foreign relations is often in flux. Over the years, OIA's teams of attorneys and paralegals have cultivated expertise and relations with the countries with whom they work. Even better, OIA attorneys have even been known to give a well-timed nudge to ensure the foreign process keeps moving.

OIA attorneys can advise whether the country where your evidence is located will be able to provide the evidence you seek informally (through police channels) or formally (such as through a Mutual Legal Assistance Treaty (MLAT) request). Depending on the country, the assigned OIA attorney may also have a network of contacts to help you obtain your evidence in the most efficient way possible. For example, in one case, a forensic copy of a hard drive seized by foreign authorities was informally and quickly made available so that the FBI could assist with decryption and share the fruits of its findings. That said, it was understood that if the original hard drive was needed for trial, an MLAT request would later be required to obtain it. Again, make sure you consult with your OIA attorney as this result might not be possible with some countries.

OIA attorneys provide advice and assistance on international criminal matters to the U.S. Attorneys' offices, the Criminal Division, other Department of Justice (DOJ) divisions, and even state and local prosecutors nationwide. They also assist other countries with their requests for assistance from the United States.

OIA's other duties include working with the Department of State to negotiate new treaties and other agreements dealing with international criminal matters. Its attorneys represent the interests of the United States by participating in multilateral convention (treaty) negotiations that are focused on a variety of law enforcement issues, such as organized crime, narcotics trafficking, terrorism, money laundering, and, yes, cybercrime. OIA attorneys can be reached by calling OIA's main number at 202-514-0000. Ask for the attorney who covers the country whose assistance you seek.

B. DOJ Attachés

DOJ Attachés, also known as Judicial Attachés, are OIA lawyers, and they serve in the U.S. Embassy in the country where they are located. Currently, there are DOJ Attachés stationed in Egypt, France, Italy, Mexico (two), the Philippines, Thailand, and the United Kingdom. The DOJ Attaché coordinates the extradition or other legal rendition of international fugitives and all international evidence-gathering for the country where the Attaché resides and, often, with other countries in the region.

Specifically, the DOJ Attaché liaises with Ministry of Justice and other relevant law enforcement counterparts on cases and can be a great resource for you and your agents. For example, in another (albeit non-cybercrime) case, a DOJ Attaché in Southeast Asia was able to provide guidance to help our investigation obtain evidence while navigating through political sensitivities. Moreover, he also was able to suggest what foreign evidence was available that would advance the investigation, and with the help of Immigration and Customs Enforcement Attachés, the agents were able to obtain copies.

As an aside, it is important to distinguish the DOJ Attachés from the Resident Legal Advisers (RLAs), our other DOJ colleagues located abroad. RLAs, based out of the DOJ's Office of Overseas Prosecutorial Development, Assistance, and Training, are tasked with developing and administering technical assistance that enhances the capabilities of foreign justice institutions and their law enforcement personnel. Their duties are not operational in scope. In contrast, the duties of the DOJ Attachés are operational in scope, and they are trained in extradition, mutual legal assistance, and other aspects of international cooperation.

C. Law enforcement agency attachés

Similarly, many U.S. law enforcement agencies have attachés—agents who are stationed abroad—who can assist with cybercrime cases. Such agencies include the FBI, ICE, IRS-Criminal Investigation, U.S. Secret Service, and others. Attachés foster a network of relationships with foreign law enforcement authorities to coordinate investigations of mutual interest. The emphasis, however, is on coordination, not on actual operations, and the rules for joint activities and information-sharing are generally formalized in agreements. In particular, because attachés are stationed abroad, they can help shorten response time when obtaining foreign assistance and in sharing investigative leads and information.

It may be helpful to note that the term "Legal Attaché" (Legat) does not refer to all attachés. Instead, it is a title established by the Department of State to refer to the special agent in charge of an FBI liaison office abroad. In addition to coordinating investigations, Legats work with their host country's law enforcement agencies. They also brief Embassy and FBI leadership, manage country clearances for their agents traveling abroad, provide situation reports concerning cultural protocol, assess political and security climates, and coordinate victim and humanitarian assistance. They also assist foreign agencies with requests for investigative assistance in the United States. Currently, the FBI has 64 Legal Attaché offices worldwide, as well as more than a dozen sub-offices, all covering more than 200 countries and territories.

Notably, FBI Legats are assisted by additional agents assigned as Assistant Legal Attachés, who sometimes have more targeted experience with cybercrime investigations. The FBI has stationed cybercrime specialists in certain European countries to assist cybercrime investigations and, in recent years, has announced its intent to expand its overseas cybercrime Assistant Legal Attaché program.

IV. MLATs and other formal mechanisms to obtain foreign assistance

Determining whether you need to use informal or formal means of seeking assistance from another country often depends on what it is that you are seeking. If you are seeking information, such as public records, you will often be able to use informal investigator-to-investigator channels to obtain this information. For example, if the other country already has an open investigation, it may be able to informally share evidence with you in order to assist with your investigation.

However, if you are seeking evidence in a form to use at trial, or need legal process to compel the production of something (such as through a subpoena or a search warrant, or when seeking the testimony of an uncooperative witness), you will normally need to use formal procedures. In fact, some countries—for example, Switzerland—even require you to go through formal processes when you reach out to

someone in their country. Failing to abide by those processes could result in facing criminal penalties in that country. OIA attorneys and the other resources discussed here can advise you about the best means to obtain the assistance you need.

Most of the time, obtaining evidence in a format ready to be used at trial requires formal cooperation. Formal cooperation can take many forms, which are primarily governed by the legal relationship that the United States has with the country in which your evidence is located. Formal cooperation can be obtained based on comity or reciprocity with another country, but assistance is discretionary in these instances. The following are some methods for formal cooperation.

A. Mutual legal assistance treaties

Perhaps the best means to obtain formal assistance is when the United States has an MLAT with another country. In this case, formal copies of evidence, such as an original hard drive or stored communications, such as emails, can be obtained by making an MLAT request.

The primary benefit of an MLAT between two countries is that it creates a treaty obligation on the countries to provide assistance to one another. (In the absence of a treaty, countries can still help each other on the basis of comity or reciprocity, but such assistance is discretionary.) The MLAT also obligates the country to keep a request and its contents confidential, limits the use of the evidence to the purposes for which it was sought, and requires that the evidence be certified in a form that allows for the evidence to be admissible in court in the requesting country, among other things.

MLAT requests are transmitted solely through each country's Central Authority, which is designated by treaty. Designating a single Central Authority eliminates confusion and streamlines the mutual legal assistance process. Moreover, the attorneys at the Central Authorities are recognized experts in mutual legal assistance. For the United States, the Central Authority for MLAT requests is OIA.

B. Multilateral conventions

If the United States does not have a bilateral MLAT, assistance can sometimes be obtained through multilateral conventions or treaties. Common examples include the United Nations Convention Against Corruption, the United Nations Convention against Transnational Organized Crime, and the several United Nations Terrorism Conventions. Each convention usually has a long list of signatory countries that are obligated to provide mutual legal assistance to other countries on the list.

Notably, each convention typically also has a set of articles that provide for mutual legal assistance, known informally as "mini-MLATs." Unlike the bilateral MLATs that are broad in scope, however, multilateral conventions are often limited in scope to the offenses that they cover (for example, corruption and bribery offenses).

C. The Budapest Convention on Cybercrime

In particular, the Budapest Convention on Cybercrime is a multilateral convention that promotes consistent laws and procedures relating to cybercrime. The Convention entered into force in 2004, and the United States joined in 2007. As of this publication, 42 countries were members. A list of member countries can be found at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF= &CL=ENG.

Generally, members agree to adopt laws criminalizing certain common crimes related to computers and the Internet, creating common procedures for investigating these crimes and preserving evidence, and providing for the protection of human rights. In fact, some countries have used the Convention as a model for their own domestic legislation. Many investigative tools parallel our own, such as preservation requests, production orders, search and seizure of stored data, real time collection of

traffic data, and interception of content. A copy of the Convention can be found at http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

Under Article 25 of the Convention, members pledge to afford each other "mutual assistance to the widest extent possible." Budapest Convention on Cybercrime, art. 25, Nov. 23, 2001. "Mini-MLAT" provisions can be found at Article 27. The bottom line is that if you need legal assistance from a country with which the United States does not have a mutual legal assistance treaty, but which is a member of the Budapest Convention, you can cite these provisions to obtain assistance for crimes set forth in the Convention.

D. Letters rogatory

If no MLAT or multilateral treaty is available, you can still obtain assistance via letters rogatory, which are a very old means of requesting assistance between countries. They are often made from a court to a foreign court, requesting that certain evidence be obtained for use in the requesting court's pending action.

Be warned: this process can take substantial amounts of time, as noted by then-Senator Christopher Dodd of the Senate Foreign Relations Committee. SPECIAL COMM. ON FOREIGN RELATIONS, MUTUAL LEGAL ASSISTANCE TREATIES WITH THE EUROPEAN UNION: REPORT, S. EXEC. REP. 110-13, at 2–3 (2008) (noting that obtaining evidence through a letter rogatory "tends to be an unreliable and time-consuming process"). Letters rogatory often require a lengthy, cumbersome authentication process called an apostille. Moreover, letters rogatory are typically transmitted to foreign judicial authorities through diplomatic channels, which itself can be a time-consuming process. Furthermore, unless required by an international agreement, compliance is a matter of judicial discretion.

E. Practice tips on preparing your formal request for assistance

Just as it is good practice to make it as easy as possible for a court to rule in your favor, it is good practice to make it as easy as possible for foreign law enforcement partners to help you get the evidence you need. A few practice tips are provided below.

- Draft MLAT requests as narrowly as possible to avoid the appearance of being overbroad, which may result in refusal of the foreign country to execute the request. Similarly, try to make your request as specific as possible. For example, if a witness needs to be interviewed, you may want to provide an extensive list of questions, rather than assume the foreign agents understand all nuances of your case.
- Use as simple language as possible. The request will usually have to be translated and a poorly written request can defeat a linguist's best efforts.
- Prepare and submit the MLAT request as early as you can. Even though the MLAT process is considered to be a relatively streamlined route, requests still take time as in-country approvals are required before the request is transmitted. Furthermore, the receiving country will need time to evaluate your request. Similarly, in fairness, foreign law enforcement agencies already have their own docket of cases, so it is understandable that they may evaluate the priority of your request differently than you would evaluate it. The MLAT process can obtain good results, but be prepared for it to take time.
- Remember that OIA can provide you with the exemplars or other tools you will need to prepare a request in line with these practice tips.

F. Assisting with other countries' requests to the United States

Over the years, many attorneys in the field have received requests from foreign countries. Although responding to these MLAT requests can take time away from your own cases, remember that providing able and prompt assistance can yield valuable connections that may assist your own investigations in the future. For example, recently, the FBI worked to assist the United Kingdom in obtaining warrants for the contents of several email accounts in time for them to be produced to the defendants there. Not only was the United Kingdom investigator pleased to report that the defendants received combined sentences of 30 years, but a valuable connection was made with an agent who was in the process of being transferred to the Cyber Crime Unit of the United Kingdom's newly formed National Crime Agency.

V. Locating your fugitive: TECS records and INTERPOL Red Notices

In situations where you do not know the location of your target, there are tools to help you locate them. For example, you can have a "lookout" placed in TECS, a system maintained by Customs and Border Protection, to notify you if your target is about to enter or leave the United States. Although it is not foolproof, good results are often possible.

You may also be able to obtain an INTERPOL Red Notice, which essentially is a request to INTERPOL's 187 member countries to "be on the lookout" for your target and to notify you if your target is located within their borders. Some INTERPOL member countries even treat a Red Notice as a provisional arrest request (described further below). Keep in mind that if your target is located, you will need to move very quickly to have him arrested, and if you need to use a provisional arrest request, the arrest triggers a deadline to have an approved extradition packet submitted to the arresting country. Red Notices, like TECS records, are not foolproof, but can often be effective.

For the United States, the INTERPOL representative is the U.S. National Central Bureau (also known as INTERPOL Washington). The Bureau's Web site can be found at http://www.justice.gov/interpol-washington/. For additional guidance and information, email INTERPOL Washington at usncb.state.mailbox@usdoj.gov, or call 202-616-9000.

VI. Arresting and returning your fugitive: extradition and other means of lawful return

Extradition is the formal legal process by which someone who is located in one country is surrendered to the requesting country for trial or punishment. It is a process generally governed by treaty. A list of countries with which the United States has extradition treaties can be found in the annotations after 18 U.S.C. § 3181. Consultation with OIA before seeking arrest or extradition is required. *See* DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-13.500 (2012).

Although every extradition treaty has different features, they nonetheless often share some commonalities. First, in order to extradite, many countries follow the principle of dual criminality, that is, the crimes for which a target is being extradited must be punishable as crimes in both countries and be punishable by more than one year imprisonment. Second, all treaties include the "rule of specialty," meaning you can only detain, prosecute, and punish your defendant for the crimes that you sought in your extradition request and the other country found to be extraditable. This is important, especially if you decide to supersede your indictment after the defendant's return to the United States. You will likely have to seek permission from the other country before including the new charges in your indictment. Consultation with OIA on these points is helpful.

For cases where it is urgent to arrest a target before he or she flees the location in which he or she is found, or in cases where your target is a danger to the community, you can make a provisional arrest request if it is permitted by the extradition treaty. (If not urgent, you typically would ask for the fugitive's

straight extradition.) Keep in mind, however, that upon arrest, the treaty requires the prosecutor to commit to provide an extradition packet within the time specified by the treaty (often, 60 days). While this period nominally provides time to prepare the formal documents, have them translated, and send the packet to the arresting country through diplomatic channels, OIA often prefers a complete extradition packet to be submitted at the same time as the provisional arrest request. This "early" submission of extradition materials to OIA ensures that all of the information necessary to support an extradition is readily at hand and that ample time is available for translation and submission of the necessary affidavits. Again, early consultation with OIA is recommended.

Start preparing your extradition request early. Be sure to write simply, bearing in mind that the packet will probably have to be translated. Be warned that you will need to present more information about your case than you probably expect. Providing more information can be a source of some frustration for prosecutors, but remember that the other country needs sufficient information to evaluate the merits of your request. For example, some countries, such as Mexico, want affidavits from witnesses.

Once you have submitted a completed extradition packet to OIA, be patient! Just as with an MLAT request, many in-country approvals may be required. Once the packet is approved, it will be conveyed via the diplomatic channels and the request will be evaluated by the other country. In some cases, the fastest scenario is if your target waives extradition. In that case, the U.S. Marshals (or your investigating agency) can retrieve your target, often within a few weeks. However, if your target chooses to resist extradition, he or she may have several layers of appeals and collateral attacks that will delay the process. Again, OIA can help by providing guidance.

Lamentably, it may not be possible for some countries to extradite your target because there is no treaty, the offense for which extradition is sought is not a crime in the foreign country (that is, no dual criminality), or for other reasons. There may be other alternatives to extradition available. For example, if your fugitive is a U.S. citizen, the other country may be able to deport your fugitive back to the United States. In other cases, if your fugitive entered a country illegally or is not admitted into the country, the country may decide to expel the fugitive back to the United States or to a country where we can seek his extradition. In yet other cases, it may be possible to use unilateral measures, that is, a lure, to have the fugitive returned to the United States or to go to a country from where we can seek extradition. Lures are legal but very sensitive techniques because they may violate the sovereignty of another country. Consequently, there are many approvals that are required, so consult with OIA for guidance.

VII. Conclusion

As cybercrimes become increasingly sophisticated, quickly preserving and obtaining evidence abroad is more important than ever. Fortunately, substantial resources are available to help you if your investigation takes you overseas.

VIII. Appendix of resources

A. Preserving Evidence via the 24/7 High Tech Network

- CCIPS is the point of contact. Call 202-514-1026 during business hours or 202-514-5000 for after hour requests, and ask for the CCIPS duty attorney.

B. MLAT requests and extraditions: the Office of International Affairs

- Call 202-514-0000, and ask for the OIA attorney assigned to the country from which you seek assistance.
- A list of member countries to the Budapest Convention on Cybercrime is available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=%20&CL=ENG.

- A copy of the Convention itself can be found at http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm.
- A list of extradition treaties with the United States can be found at the end of 18 U.S.C. § 3181, but make sure to consult with OIA.

C. INTERPOL Red Notices

- The Web site for INTERPOL Washington is available at http://www.justice.gov/interpol-washington/.
- For additional guidance and information, email INTERPOL Washington at usncb.state.mailbox@usdoj.gov, or call 202-616-9000. ❖

ABOUT THE AUTHOR

❑ **Michael Chu** is an Assistant U.S. Attorney who recently returned to Texas to join the U.S. Attorney's Office in Houston. Before that, he worked in the white collar section of the U.S. Attorney's Office in Las Vegas, where he also served for six years as the computer hacking and intellectual property coordinator. ✠

The author would like to thank Jeff Olson, Betty Shave, Tim O'Shea, Ed Gallagher, Edward Ng, and Jason Smith for their contributions to this article, as well as every OIA attorney with whom he has ever worked.

Overcoming the Unique Challenges Presented in "Time Bomb" Computer Intrusion Cases

Mark L. Krotoski
Assistant Chief
National Criminal Enforcement Section
Antitrust Division

Consider the following facts: John is an executive who works at a growing company with an emerging product. For the past week, he has been traveling out of the country on a business trip. He arrives at work early Monday morning, when he learns for the first time that hundreds of thousands of company records were systematically deleted over the weekend. The attack started while he was traveling on a long flight back, when he was unreachable. The IT Department responded quickly but has not yet been able to determine the source of the attack. Private contractors working with the company on network issues were incident responders and immediately assisted. A team of company officials and outsiders is assembled and tasked to determine the cause of the attack. Initial signs suggest that a time bomb may have been planted on the network and was designed to cause significant damage and harm. There is no other explanation for how so many sensitive records could have been destroyed. Whoever was responsible appears to be familiar with the company network as the malicious code exploited some key

network vulnerabilities. The company is momentarily paralyzed as employees are denied access to the network until further information can be obtained. Based on what is known so far, the company decides to report the incident to law enforcement.

These hypothetical facts present a common scenario when a time bomb (sometimes referred to as a "logic bomb") has been placed on a computer network. Unlike other computer intrusion offenses, time bomb cases present some unique issues and challenges. The use of time or logic bombs is periodically in the news. *See, e.g.*, Kim Zetter, *Logic Bomb Set Off South Korea Cyberattack*, WIRED (Mar. 21, 2013) ("A cyberattack that wiped the hard drives of computers belonging to banks and broadcasting companies in South Korea this week was set off by a logic bomb in the code, according to a security firm in the U.S."), *available at* http://www.wired.com/ threatlevel/2013/03/logic-bomb-south-korea-attack/. As noted below, there have been a number of successful time bomb investigations and prosecutions. *See infra* Part X (summarizing cases).

This article will review some of the unique obstacles that arise in time bomb cases. The article also identifies some key recurring issues and recommends five specific steps that may assist in addressing and overcoming the challenges in this distinct type of computer intrusion case.

I. What is a time bomb?

A time bomb is a unique form of a computer intrusion. Typically, a time bomb is carefully designed to cause significant damage to a computer network at a predetermined time or event. Malicious code or software may be planted by someone with familiarity with the network or company operations. Usually, it is an insider who knows enough about the vulnerabilities of the network and is motivated by anger or some dispute.

One definition that captures the operation of a logic or time bomb provides:

> Logic Bomb: A logic bomb is a type of malware that executes a set of instructions to compromise information systems based on the logic defined by its creator. Logic bombs are usually programs that use either time or an event as the trigger. When the condition(s) stipulated in the instruction set is met, the code present in its payload is executed. It is mostly used by disgruntled employees planning revenge on their employers or by Blackhats hackers for financial gains.

AMAN HARDIKAR, MALWARE 101—VIRUSES 7 (SANS Institute 2008), *available at* http://www.sans.org/reading-room/whitepapers/incident/malware-101-viruses-32848.

II. Unique challenges

Time bomb investigations and cases present unique issues that do not arise in other computer intrusion or cyber cases.

A. Insider

Many computer intrusion cases involve external acts. Someone outside a company hacks into the company network remotely. In contrast, many time bomb cases are typically an inside job. For example, the defendant may plant the bomb on the network after he learns he will be terminated or as he departs the company over a dispute. *See, e.g.*, *United States v. Lloyd*, 269 F.3d 228, 236 (3d Cir. 2001) (noting Government's trial theory that the defendant, "before he was terminated from his employment . . . sabotaged the computer system," reversing grant of motion for a new trial, reinstating the conviction, and directing that the trial court proceed to sentencing). While time bombs may also be committed by outsiders to the network, this is less common.

B. Intimate familiarity with the network

Someone familiar with the company network plants a malicious code, which is set to destroy a number of records or commit some other malicious act. The gravity of the harm may result from the insider's familiarity with where the sensitive information may be located.

C. Alibi issues

It may be difficult to determine who is responsible for the time bomb, particularly when the execution may have been designed to prevent detection of the person planting it. The offense is normally committed by someone with a sophisticated understanding of the company network and computer issues. The perpetrators may have planned what they believe is a perfect alibi, launching the time bomb after they have left the company.

D. Concealment

Most likely, steps have been taken to conceal the offense and trail of evidence. In destroying records, obstruction of justice may apply. The individual may have left the company and moved on and may even have a planned alibi, as mentioned above.

E. Technical evidence

Much, if not most, of the evidence may be electronic and highly technical, raising questions about the presentation of the evidence and ability of the jury to follow it. Experts may be required to understand the operation of the malicious code or software. The difficulty in finding the code may be exacerbated if steps to delete it were made. Much of the evidence may be circumstantial.

This article reviews recent time bomb cases and some of the lessons learned in investigating and prosecuting these cases.

III. Common charge to consider: 18 U.S.C. § 1030(a)(5)(A)

In terms of charges, most often the intentional computer damage provision of 18 U.S.C. § 1030(a)(5)(A) will be utilized. This provision punishes anyone who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A) (2014).

The Ninth Circuit jury instruction provides an example of the elements for this offense:

> First, the defendant knowingly caused the transmission of [a program] [a code] [a command] [information] to a computer;
>
> Second, as a result of the transmission, the defendant intentionally impaired without authorization the [integrity] [availability] of [data] [a program] [a system] [information];
>
> Third, the computer was [exclusively for the use of a financial institution or the United States government] [used in or affected interstate or foreign commerce or communication] [located outside the United States but was used in a manner that affects interstate or foreign commerce or communication of the United States] [not exclusively for the use of a financial institution or the United States government, but the defendant's transmission affected the computer's use by or for a financial institution or the United States government]; and
>
> Fourth, the impairment of the data, program, system or information resulted in either (a) loss to one or more persons aggregating at least $5,000 in value during the one-year period following the date of the impairment; (b) the modification or impairment, or

> potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals; (c) physical injury to any person; (d) a threat to public health or safety; (e) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or (f) damage affecting 10 or more protected computers during any one-year period.

18 U.S.C. § 1030(a)(5)(A) (modified to include fourth felony element) (2014); NINTH CIRCUIT MANUAL OF MODEL CRIMINAL JURY INSTRUCTIONS § 8.100—Intentional Damage To A Protected Computer, *available at* http://www3.ce9.uscourts.gov/jury-instructions/node/558.

A misdemeanor results under the first three elements for § 1030(a)(5)(A). The fourth element makes the offense a felony under §§ 1030(a)(5)(A) and 1030(c)(4)(B)(i) (felony penalty provision). Sections 1030(b) and 1030(c)(4)(B)(ii) punish an attempted violation of § 1030(a)(5)(A) in the same manner.

For time bomb cases charging a violation of § 1030(a)(5)(A), consider: *United States v. Makwana*, 445 F. App'x 671, 674 (4th Cir. 2011) (per curiam) (affirming time bomb jury trial conviction of a UNIX engineer working as a contractor at Fannie Mae, under §§ 1030(a)(5)(A)(i), (B)(i), (c)(4)(A)); *United States v. Shea*, 493 F.3d 1110, 1112 (9th Cir. 2007) (affirming the jury trial conviction of a system administrator who planted a "time bomb" on the company network after becoming disgruntled at work, under § 1030(a)(5)(A)(i)); *United States v. Sullivan*, 40 F. App'x 740, 744 (4th Cir. 2002) (per curiam) (affirming conviction of computer programmer who inserted a "logic bomb" into the software for Lance, under § 1030(a)(5)(A)); *United States v. Lloyd*, 269 F.3d 228 (3d Cir. 2001) (reinstating the trial conviction of a former computer network administrator at Omega Engineering Corporation, under § 1030(a)(5)(A)); *United States v. Duchak* (D. Colo. 2010) (No. 10-CR-131-MSK) (plea agreement conviction of a data analyst working as a government contractor at the Transportation Security Administration, under §§ 1030(a)(5)(A), 1030(b), and 1030(c)(4)(B)); *United States v. Yung-Hsun Lin* (D.N.J. 2007) (No. 06-cr-00963-JLL) (plea agreement conviction of former computer systems administrator for Medco Health Solutions, Incorporated, under §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(c)(4)(A), 1030(b)); *United States v. Roger Duronio* (D.N.J. 2006) (No. 02-CR-00933-JLL) (jury trial conviction of former systems administrator at UBS Paine Webber, under §§ 1030(a)(5)(A)(i), 1030(c)(4)(A) and one count of securities fraud). The background and outcome in these cases is summarized in Part X below.

With these elements in mind, the most challenging area of proof typically involves the first element: establishing that the defendant knowingly caused the transmission of the code or program. This challenge may stem in part from efforts taken by the defendant to conceal the time bomb activity. The second element, intended impairment of a network, usually was the objective for designing the time bomb. The evidence will readily establish that the malicious code resulted or was designed to cause substantial harm. For most businesses, the third element, showing that the computer was either used in or affected interstate or foreign commerce or communication or was used by a financial institution, is readily established.

Finally, establishing the loss resulting from the impairment usually can be proven by showing the intended impact (how the time bomb was designed) and the actual resulting harm. Section 1030(e)(11) defines "loss" as including "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11) (2014). Section 1030(e)(8) further defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." *Id.* § 1030(e)(8). The term " 'government entity' includes the Government of the

United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country." *Id.* § 1030(e)(9).

Depending on the facts, other offenses may include § 1030(a)(5)(B) (causing damage recklessly), § 1030(a)(5)(C) (causing damage (and loss) negligently), or § 1030(a)(4) (computer fraud, for example, if a misrepresentation was used to commit the offense).

IV. Obtaining the electronic records

Since the offense was likely committed on a computer network, much of the evidence will consist of electronic records. The initial steps in the investigation may therefore be among the most important.

The company will likely be scrambling to mitigate the damage, maintain business operations, and determine the cause. The company will also likely assign a team to investigate the circumstances and may have started its own forensic analysis and assessment of the cause of the damage.

Some time may elapse before more is known and a company decision can be made as to whether to contact law enforcement. Consequently, the processing of electronic evidence may not be handled by law enforcement for a substantial period of time. By the time law enforcement arrives, the electronic records may no longer be in the same condition as they were shortly after the incident. However, when law enforcement does arrive, it normally receives the results of the company's internal investigation and will need to complete an independent review of the evidence as part of the law enforcement investigation. The company also may have backup tapes, which may be useful in analyzing and restoring, if possible, the electronic records.

V. Five-step process: operation, access, ability, knowledge, motive

After the company has contacted law enforcement, assume you have been asked to assist in the investigation and prosecution of a reported time bomb. Initially, there may be a handful of primary subjects within the scope of the investigation. What steps can be taken to focus on the most likely candidates? How will you prepare for anticipated defenses which may include an alibi defense or claims that someone else did it?

Given that some level of disgruntlement may have supplied a motive to plant the time bomb, there may be labor dispute issues between the key suspects either currently or formerly employed by the company. Will those issues distract from the presentation of the evidence at trial?

In confronting these challenges, certain lessons can be drawn from time bomb investigations and cases. In particular, a five-step process has been utilized in handling past time bomb investigations and prosecutions. This process has proven useful to identify the primary perpetrators and to present and focus the trial evidence. The five steps include determining: (1) how the time bomb *operated*, (2) what *access* was necessary to plant and execute the time bomb, (3) who had the *ability* to prepare and use the time bomb, (4) who had the *knowledge* (or familiarity) to tailor the time bomb to the company network or records, and (5) who had the *motive* to install and launch the time bomb, particularly given the specific type of harm caused.

A. Operation of the time bomb

Initially, investigators need to learn as much as possible about the time bomb. This information will provide clues about the capabilities of the perpetrators and identify new leads. Some initial questions may include:

- How was the time bomb designed to operate?
- Were any particular programming languages used for the source code?

- Were any signature aspects noted in the manner in which the time bomb code was written (e.g., unique or specific commands)?
- Was any proprietary code necessary?
- How did the time bomb interface with the network and system on which it was planted?
- What steps to test the time bomb may have been taken?
- What planning and preparation may have been necessary?
- When and how was the time bomb planted onto the system?
- What was the triggering event for the time bomb (for example a date and/or event)?
- What significance is there to the triggering event or date?
- Were steps taken to wipe or delete evidence?

The initial answers to these and other relevant questions will help focus on the individual(s) who had the means to design and launch the time bomb.

B. Access

Once information is obtained about the operation of the time bomb, a second key issue concerns access. In order to launch the time bomb, what access was required? Was access made remotely, such as through a company laptop or by hackers, or was access made from inside the company?

The access point may provide some key evidence leads about the commission of the offense. Other questions to consider may include:

- Were particular computers used to access the network?
- Was access within or outside the company?
- If remote access was made, how is access to the network obtained? How many steps are involved?
- What credentials or passwords are required to obtain network access?
- How many passwords are needed to obtain access (for example, one password to use a computer and a separate password to visit certain network areas)?
- For password usage, who determines the password? Does the user choose or does the company assign a password? What is the company policy on how frequently the passwords for each level necessary to obtain access must be changed?
- Are any company policies concerning computer security implicated in assessing how access was made?
- How many computers do the likely suspects have assigned? Is there evidence of planning, preparation, or testing of the time bomb on other devices?
- Was any proprietary program or software involved?

Access may include physical and network levels. On the physical level, if the investigation shows that a particular computer was used to plant and launch the time bomb, what physical access is required to get to that computer? Are there security measures that restrict outsiders from entering the company or areas of the company? Is there a sign-in log for visitors? Do key card records show the date and time of access of individuals to a particular area where the computer was located?

Separate from physical access is network access. It may be that access to the network where the time bomb was launched requires multiple passwords. For example, an initial password may be necessary to operate the computer. Other passwords may be required to visit certain locations on the network. Log records may demonstrate the date and time for this type of network access.

Normally the five-level process (operation, access, ability, knowledge, motive) can be used collectively to narrow the list of suspects responsible for the time bomb. Usually, more than access is required to identify the primary perpetrator of the time bomb attack. However, the *Duchak* time bomb case provides an example of how the access evidence was used to confirm the defendant's involvement. The stipulated factual basis of the plea agreement provided:

> Mr. Duchak's work station, together with those of other CSOC [Colorado Springs, Colorado] employees, were located in an office space whose entrance was monitored by video surveillance and secured doors that could be accessed only though use of an electronic card reader, keypad (with unique user access code) and thumb print scan.

A subsequent internal investigation, including review of video surveillance of the CSOC entrance, computer logs, and records generated at the secured door (card swipe, keypad access, and thumb print) showed that:

> (1) On October 23, 2009, Douglas James Duchak returned to the CSOC after business hours, and remained there between approximately 6:59 p.m. and 8:11 p.m.
>
> (2) Once inside, the defendant logged on to his work station using his network credentials and input computer code that directed, in essence, "if date is November 3, 2009, then no fly list will be replaced with TSDB" (the Code V). The defendant then copied the Code from his work station to a server at the CSOC.

Had this Code operated on November 3, 2009, its effect would have been to replace a much smaller file with a much larger file and thereby prevent new data from being properly updated into the TSDB and temporarily disable the Transportation Security Administration's vetting function.

> (3) The defendant then logged off his own work station; logged on to the work station assigned to N.l. using the defendant's credentials, and copied the Code from the CSOC server to N.l.'s work station.

United States v. Duchak (D. Colo. 2010) (No. 10-CR-131-MSK) (plea agreement factual basis stipulation) (Doc. No. 70).

C. Ability

A third issue concerns ability. Access alone is likely to be insufficient for a successful time bomb attack. Ability is typically required to design and plant the time bomb on the network. *See, e.g.*, *United States v. Lloyd*, 269 F.3d 228, 234 (3d Cir. 2001) (Government argument that only the defendant possessed certain "system administrative skills, programming skills, Microsoft Windows experience, and independent knowledge of how to change the deleting program's message" to commit the time bomb); *see also United States v. Shea*, 493 F.3d 1110, 1117–18 (9th Cir. 2007) (noting the defendant's "ability to program in the Unix database and in the Collector System files" used in the time bomb was "undisputed and appears to have been unique among" company employees).

Once information is obtained about how the code operated, how it was planted, how it was set off, and what type of ability was necessary? Some initial questions that may be relevant concerning ability may include:

- What skills are necessary to design, implement, and launch the time bomb?

- What special programming skills may be necessary?
- What other skills are required given the computer network system?
- Was any proprietary code or information involved?
- Which primary suspects have this ability?
- Are there any signature attributes in the manner in which the programming language for the malicious code was written? If so, how do they compare to other work of the suspect?
- What does the defendant's or suspect's resume (or other employment papers) show about the abilities necessary to execute the time bomb?

D. Knowledge

Access and ability alone may be insufficient for a successful time bomb attack. Knowledge about the network and files is also required. The manner in which the time bomb was planted and operated likely entails intimate familiarity with the files and networks. Few individuals may have this knowledge or familiarity.

The familiarity that the perpetrator had about the network may reveal how he could exploit unique network vulnerabilities. The list of suspects will further be narrowed by considering who had access, ability, and knowledge to plant and launch the time bomb.

Some questions to consider may include:

- How was the malicious code designed to destroy particular company files or records?
- Were any proprietary or unique company names used in the malicious code?
- How did the perpetrator know which company files and records to access?
- What does the network location in which the time bomb was planted reveal about familiarity with the company computer system?
- How many individuals have this level of familiarity and knowledge?

E. Motive

Finally, as a fifth aspect, there is usually a motive that provides the basis for an individual to plan, prepare, and launch the time bomb.

A number of the cases involve termination or labor disputes. *See, e.g.*, *United States v. Shea*, 493 F.3d 1110, 1112–13 (9th Cir. 2007) (defendant convicted at trial for planting a "time bomb" on the company network after engaging in employment disputes, being placed on a "performance plan," and being terminated for failing to come to work); *United States v. Sullivan*, 40 F. App'x 740, 741 (4th Cir. 2002) (per curiam) ("Sullivan then quit without telling anyone about the bomb. The bomb went off about four months later, disabling 824 hand-held computers used by Lance's sales representatives to communicate with the headquarters."); *United States v. Lloyd*, 269 F.3d 228, 232 (3d Cir. 2001) ("The government argued at trial that the demotion, along with the substandard performance review and raise, indicated to Lloyd that he would soon be fired, thus providing him with the motive to sabotage Omega's computer system."); *United States v. Rajendrasinh Babubahai Makwana* (D. Md. 2010) (No. 09-cr-00043) (defendant convicted at trial for malicious code transmitted following termination that was designed to execute on Fannie Mae computer network three months later).

Some key questions may include:

- If the time bomb appears to be the work of insiders, was the employee terminated or did the employee leave on unfriendly terms? Was the employee placed on a performance improvement plan?
- Was an exit interview conducted prior to the employee's departure?
- What statements did the suspects make to others concerning his or her views of the company?
- What happened days and weeks before the time bomb was planted on the system that may demonstrate an escalating dispute or misunderstanding?
- Were any performance review meetings held prior to the time bomb and what happened at these employment meetings?
- Once a time line of key events is developed, how do labor dispute issues fit on the time line?

The answers to these questions will highlight new evidence leads. For example, if there was an employment dispute, the investigation can focus on the events surrounding the dispute. Did the suspect make angry statements about harming the company? Did the suspect confide in others his contempt of company management?

F. Process used to narrow and identify likely suspects

This five-part process, which has been used in prior cases, will help focus the investigation on identifying the likely suspects. The list of suspects who may be responsible for the time bomb will be narrowed depending on who had the access, ability, knowledge, and motive. The five steps will help identify key evidence for the investigation and possibly new leads. Once the key evidence is obtained, the five-part process will help formulate a timeline to use at trial and will focus the presentation of the trial evidence and rebutting of defense claims.

VI. Key anticipated defenses

Most of the time bomb defenses are typically based on claims that someone else committed the offense or some other occurrence caused the computer damage.

A. Someone else did it

Given that the time bomb was designed to be triggered by a particular date and/or event, it is not uncommon for the theory of defense to be that someone else was responsible. For example, the time bomb may have been planted while the defendant was still employed at the company, but executed on a date following his termination. *See, e.g.*, *Shea*, 493 F.3d at 1117 (The defendant "was apprised of his termination at the office on Monday, January 20. [Time bomb] CLEAR.CF.MARKS allegedly triggered early in the morning January 30."); *Lloyd*, 269 F.3d at 233 (The defendant was terminated based on an employment dispute on July 10, 1996, and the time bomb was detected on July 31, 1996.).

Illustratively, this claim was made in the circumstantial time bomb trial in *Shea*. In that case, the Ninth Circuit noted:

> Shea also argues that several other BACS [Bay Area Credit Services] employees had access to his computer or could have logged on as him remotely. He presented evidence to the jury that another BACS employee was logged in from Shea's desktop computer at all the relevant times. However, given Shea's level of access, which included access to the Unix names and passwords of all other BACS employees, and given Shea's tendency to open multiple sessions at once from his computer, operating from both his laptop and desktop computers, a juror could reasonably infer that Shea had logged in as the other employee during all the relevant times. Because the prosecution "need not affirmatively

> rule out every hypothesis except that of guilt," *Wright v. West*, 505 U.S. 277, 296 (1992) (internal quotation marks omitted), we find that reasonable inferences from this record support Shea's conviction.

Shea, 493 F.3d at 1117–18. The multiple process factors (access, ability, knowledge, motive) were useful in showing there was sufficient evidence to support the conviction on appeal. As the Ninth Circuit concluded:

> Viewing the evidence in the light most favorable to the prosecution, with all reasonable inferences that can be drawn from the record, we hold that a rational juror could have found Shea guilty. His access to the relevant files is undisputed. His ability to program in the Unix database and in the Collector System files is undisputed and appears to have been unique among BACS [Bay Area Credit Services] employees. His antagonistic relationship with BACS executives provided him with a motive, and the timing of certain edits corresponds with the meetings and e-mails that preceded his termination.

Id. at 1117.

B. Another source caused the computer damage

The defense may also try to argue that the computer damage was caused by accident or some other occurrence. As an example, this argument was presented at trial in the *Lloyd* case:

> The defense's theory was that the massive deletion of files could have resulted from an accident or could have been caused by another employee, either intentionally or unintentionally. The defense contended that Lloyd could not have committed the act of sabotage because he did not have direct access to the system after he was fired and because he had no motive before he was fired, as his firing was without warning.

Lloyd, 269 F.3d at 231.

In response, the Government focused on the facts of the case, which showed: (1) that "the specificity of the commands" were inconsistent with "accidental deletion[s]," (2) that "the exact same strings of commands" used in the time bomb were located on a hard drive obtained from the defendant's residence, (3) that the time bomb had been tested "on three separate occasions" when the defendant was at work, and (4) the date on which the time bomb was planted. *Id.* at 234. The Government's evidence at trial showed how the details about the manner in which the time bomb was executed, along with other facts, can be used to counter an accidental damage theory or claim that another source may be responsible. The jury rejected this defense and convicted the defendant.

C. Consider a Rule 12.1(a)(1) request for an alibi notice

If it is anticipated that the defense will claim that someone else committed the offense, a Request for an Alibi Notice under Federal Rule of Criminal Procedure 12.1 should be considered. As noted by the rule drafters, "The objective of rule 12.1 is to prevent [surprise] by providing a mechanism which will enable the parties to have specific information in advance of trial to prepare to meet the issue of alibi during the trial." FED. R. CRIM. P. 12.1 advisory committee's note (1974). *See generally Williams v. Florida*, 399 U.S. 78, 81–82 (1970) (noting that because an alibi defense is easily "fabricated," the Government's "interest in protecting itself against an eleventh-hour defense is both obvious and legitimate," adding that defendants must know that a criminal trial "is not . . . a poker game in which players enjoy an absolute right always to conceal their cards until played").

The provisions of the rule are triggered by the Government's request. Under Rule 12.1(a)(1), a prosecutor submits a written request that the defendant provide notice whether an alibi defense is intended. The request "must state the time, date, and place of the alleged offense." FED. R. CRIM. P.

12.1(a)(1). The defense must respond within 14 days of the Government's request, including detailed information about "(A) each specific place where the defendant claims to have been at the time of the alleged offense; and (B) the name, address, and telephone number of each alibi witness on whom the defendant intends to rely." *Id*. 12.1(a)(2)(A), (B). After the defense responds with this information, the Government must provide information about witnesses that undermine an alibi theory under Rule 12.1(b)(1). There is a continuing duty of disclosure under Rule 12.1(c).

The failure to provide notice may result in the exclusion of a defense alibi witness. *See* FED. R. CRIM. P. 12.1(e) (providing that "a court may exclude the testimony of any undisclosed" alibi witness if a party does not comply with the Rule's requirements); *see also United States v. Acosta-Colon*, 741 F.3d 179, 187–90 (1st Cir. 2013) (affirming exclusion of the defendant's wife as an alibi witness based on a failure to comply with the rule); *United States v. Ford*, 683 F.3d 761, 764 (7th Cir. 2012) ("Notice to the prosecution of proposed alibi evidence is required because an alibi defense is at once compelling if accepted and easy to concoct, so the prosecution is justified in wanting an opportunity to investigate it in advance of trial. . . . And so the district judge was right to exclude the evidence because of the defendant's failure to have complied with Rule 12.1(a).") (citations omitted); *United States v. Nelson-Rodriguez*, 319 F.3d 12, 35–36 (1st Cir. 2003) (affirming exclusion of alibi evidence based on untimely notice under Rule 12.1).

Rule 12.1 provides useful procedures to mitigate any surprise alibi defense at trial. Given the nature and design of time bombs to launch on the occurrence of an event when the defendant may not be at the company, this process will be helpful to prepare for these issues at trial.

Prosecutors may want to consider separate levels of alibis: a physical one and an electronic one. The physical alibi request will focus on where the defendant or other suspects or individuals were at key times and events in the planning, preparation, planting, and launching of the time bomb. The electronic alibi would focus on where the defendant and others were in terms of the transmission of the codes and commands connected with the time bomb.

VII. Charging obstruction of justice

Some time bomb cases may present obstruction of justice issues. For example, steps may have been taken to conceal or destroy evidence so investigators could not find it. If so, one possible charge would include 18 U.S.C. § 1519, which provides:

> Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.

In 2002, Congress enacted Section 1519 as part of the Sarbanes-Oxley Act. *See* Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 802(a), 116 Stat. 800 (July 30, 2002) (codified at 18 U.S.C. § 1519 (2014)).

This provision was expressly drafted to apply to the destruction of records prior to the commencement of an actual investigation, as long as it can be established that the destruction was conducted in anticipation of a federal investigation. As explained in the Senate Report:

> Other provisions, such [as] 18 U.S.C. § 1503, have been narrowly interpreted by courts, including the Supreme Court in *United States v. Aguillar*, [515 U.S. 593,] 115 S. Ct. 593 (1995), to apply only to situations where the obstruction of justice can be closely tied to a pending judicial proceeding. . . . In short, the current laws regarding destruction of evidence are full of ambiguities and technical limitations that should be corrected. This provision is meant to accomplish those ends.

> Section 1519 is meant to apply broadly to any acts to destroy or fabricate physical evidence so long as they are done with the intent to obstruct, impede or influence the investigation or proper administration of any matter, and such matter is within the jurisdiction of an agency of the United States, or such acts done either in relation to or in contemplation of such a matter or investigation. . . . It also extends to acts done in contemplation of such federal matters, so that the timing of the act in relation to the beginning of the matter or investigation is also not a bar to prosecution. The intent of the provision is simple; people should not be destroying, altering, or falsifying documents to obstruct any government function.

S. REP. NO. 107-146, at 14–15 (2002).

Generally, the elements of proof for Section 1519 will include: "First, the defendant knowingly altered, destroyed or concealed a record or document; and Second, the defendant acted with the intent to impede, obstruct or influence the investigation of a matter by or within the jurisdiction of the Federal Bureau of Investigation which he either knew of or contemplated." *United States v. Kernell*, 667 F. 3d 746, 753 n.3 (6th Cir. 2012). If there is sufficient evidence to show that the defendant intended to impede an anticipated investigation by the destruction of records about the time bomb or evidence that may identify the perpetrator, Section 1519 may be considered as an appropriate additional charge.

VIII. Trial issues

Much of the evidence is likely to be electronic, such as network logs and computer code. Will the jury be able to follow the technical evidence?

A. Expert testimony

Expert testimony will likely be necessary to help the jury understand the evidence, including how the time bomb was found, how it operated, and how it caused damage to the system. In addressing these issues, potential experts may include network specialists, programming language experts to explain how the malicious code was designed to operate, and forensic examiners.

Some candidates for expert testimony may include company officials or the first incident responders who assisted in assessing the source and cause of the damage. Law enforcement officials can provide expert testimony about the forensic examination and how certain log or other electronic records were obtained. Given the technical nature of much of the evidence, care must be taken to identify the best experts to assist the jury in understanding the evidence.

B. Role of visual evidence for the jury

Much of the evidence will include electronic evidence. Some of the electronic evidence can be highly technical and difficult to comprehend. How can the essence of this evidence best be communicated to the jury? Visual diagrams of the network may illustrate to the jury where the time bomb was planted and launched. Visuals may aid the jury in understanding how certain commands in the malicious code operated. The investment of time in brainstorming the best visual exhibits will be worthwhile to overcome and explain technical issues in the case.

C. Using a timeline

Consider a timeline to focus on the unfolding events and highlight the key issues demonstrating the defendant's involvement. The timeline can illustrate the planning and preparation and any testing of the time bomb before it was planted and executed.

The timeline will also be useful in showing motive and intent. For example, the timeline may also juxtapose motive evidence, including any performance review meetings, employment warnings, and terminations. Key statements by the defendant can be added to the timeline.

Finally, the timeline may also be helpful in responding to any issues raised on appeal. *See, e.g.*, *Shea*, 493 F.3d at 1115 ("At Shea's trial, the prosecution constructed a timeline for the two relevant programs . . . ."); *id*. at 1116–17 (summarizing timeline).

D. Avoiding diversionary issues

In many time bomb cases, there may be a cloud of issues surrounding any labor dispute. While some labor dispute evidence may be relevant to show motive, the defense may seek to introduce additional evidence to seek sympathy from the jury over the employment issues. The Federal Rules of Evidence can be used to maintain focus on relevant issues under rules 401 and 402, and avoid evidence that risks "unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence" under rule 403. *See* FED. R. EVID. 401–03. The case should necessarily focus on who intentionally caused computer damage under 18 U.S.C. § 1030(a)(5)(A), and not on the merits of any labor dispute.

The defense likely will seek to confuse the jury on the technical issues. Consequently, it is imperative to focus on what the electronic records established in the case. Here is an example in which the defense tried to suggest that others with root level access may have had access to the network and could have been responsible for the time bomb. During extensive defense cross-examination of the government network expert, defense counsel suggested that anyone with root level access could be responsible, and a number of company officials had root level access. On redirect, the expert was asked:

> Question: So you were asked about 35 minutes of questions about root access. How do those questions relate to the evidence that you have reviewed concerning the access and the modification of the malicious time bomb in this case?
>
> Answer: The evidence I found didn't show that the changes were made by the actual root user.

United States v. William Carl Shea, Trial Transcript, 387 (N.D. Cal. 2005) (No. CR 03-20057-RMW). It also helps to focus on the type of records that would be created under the defense version of events and determine whether those records confirm the defense theory. The following demonstrates this point:

> Question: If someone accesses the network by root level access, what types of logs or records are created?"
>
> Answer: Normally, a log record is created, a command stack record is made, and separate passwords are used for this access.
>
> Question: Did you find records consistent with root level access for the time bomb in this case?
>
> Answer: None of the records I mentioned were found.

Id. Trial Transcript, 590-91 (modified for clarity). The computer records may also confirm the defendant's connection to the time bomb activity:

> Question: Did you review the digital evidence in this case to determine whether there was any super user access?
>
> Answer: Yes.
>
> Question: And what did you determine based on that review?

Answer: The only super user access at that time was from [the defendant] and accounts assigned to him. The other times of access did not involve super-user access.

Id. Trial Transcript, 712-13. These examples show how the electronic records can respond to defense efforts to confuse or divert the jury's attention on technical issues, or reconfirm the defendant's role concerning the time bomb.

IX. Sentencing issues

A number of sentencing issues arise in time bomb prosecutions. This overview highlights some common issues:

Base Offense Level [U.S.S.G. § 2B1.1(a)(2)]	6
Amount of Loss [U.S.S.G. § 2B1.1(b)]	+ ?
Intentional damage [U.S.S.G. § 2B1.1(b)(18)(A)(ii)]	+4
Sophisticated Means [U.S.S.G. § 2B1.1(b)(10)(C)]	+2
Special Skill/Abuse Of Trust [U.S.S.G. § 3B1.3]	+2
Factors under 18 U.S.C. § 3553(a)	

As with most intrusion cases, a portion of the sentence will be based upon the loss under the Sentencing Guidelines table, pursuant to U.S.S.G. § 2B1.1(b). As explained in application note 3(a)(v)(III),

> actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.

U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. n.3(a)(v)(III) (2014).

A conviction under 18 U.S.C. § 1030(a)(5)(A) results in a four-level increase under U.S.S.G. § 2B1.1(b)(18)(A)(ii). *See, e.g.*, *United States v. Douglas James Duchak* (D. Colo. 2010) (No. 10-CR-131-MSK) (plea agreement stipulation to four level enhancement under §2B1.1(b)(16)(A)(ii)) (Doc. No. 70); *United States v. Yung-Hsun Lin* (D.N.J. 2007) (No. 06-cr-00963-JLL) (plea agreement stipulation to four level enhancement under prior § 2B1.1(b)(14)(A)(ii) (for a violation of 18 U.S.C. § 1030(a)(5)(A)(i), increase by 4 levels)) (Doc. No. 16).

Abuse of a position of trust and use of a special skill to commit the offense may result in a two-level enhancement under U.S.S.G. § 3B1.3. *See e.g.*, *Duchak*, (plea agreement stipulation to two level enhancement under §3B1.3) (Doc. No. 70).

Another two-level enhancement may apply for an offense involving "sophisticated means" under § 2B1.1(b)(10)(C). Under the guidelines, this typically "means especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense." U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. n.9 (2014). *See, e.g.*, *United States v. Makwana*, 445 F. App'x. 671, 673 (4th Cir. 2011) (per curiam) ("Although not every aspect of Makwana's scheme was complex or intricate, we easily conclude that, viewed as a whole, Makwana's mode of access to the Fannie Mae server in which he

embedded malicious code, coupled with his efforts to conceal the presence of the code and his connection to it, were unambiguously sophisticated.").

Depending on the facts, other sentencing enhancements may apply:

- *Financial Institution*: Four-level enhancement under U.S.S.G. § 2B1.1(b)(16)(B)(i) because the offense substantially jeopardized the safety and soundness of a financial institution. *See also, e.g.*, *Makwana*, 445 F. App'x. at 674 ("The district court's findings make clear that Makwana's offense conduct jeopardized Fannie Mae's soundness by exposing the entity to the non-illusory risk of losing all of the data stored on its computer servers. Although the malicious code was discovered and removed before the date it was programmed to execute, it was not necessary to the application of Makwana's enhancement that the data on the servers be actually deleted.").
- *Risking Death and Serious Bodily Injury*: Two-level enhancement under U.S.S.G. § 2B1.1(b)(15)(A) for consciously and recklessly risking death or serious bodily injury. *See, e.g.*, *United States v. Yung-Hsun Lin* (D.N.J. 2007) (No. 06-cr-00963-JLL) (plea agreement stipulation to two level enhancement under prior § 2B1.1(b)(12)) (Doc. No. 16).

Finally, as with any sentence, the court will consider the sentencing factors under 18 U.S.C. § 3553(a).

X. Other time bomb case examples

There have been a variety of successful time bomb prosecutions over the past several years. Some cases have been resolved by pleas. Others have resulted in jury convictions. As examples, the background and outcome of some of these time bomb cases are summarized below:

- *United States v. Rajendrasinh Babubahai Makwana*, (D. Md. 2010) (No. 09-CR-00043): A jury convicted the defendant, who was a UNIX engineer working as a contractor at Fannie Mae, for transmitting malicious code that was designed to destroy all data on network computers, including financial, securities, and mortgage information, following his termination, in violation of 18 U.S.C. §§ 1030(a)(5)(A)(i), (B)(i), (c)(4)(A). The code was designed to execute three months later. He was sentenced to serve 41 months in prison. His conviction and sentence were affirmed on appeal. *See United States v. Makwana*, 445 F. App'x. 671(4th Cir. 2011) (per curiam). *See also* Thomas Claburn, *Fannie Mae Contractor Indicted For Logic Bomb*, INFO. WEEK (Jan. 29, 2009) ("Had the malicious script designed to wipe Fannie Mae's 4,000 servers not been discovered, the company could have lost millions of dollars and a week's worth of uptime."), http://www.informationweek.com/traffic-management/fannie-mae-contractor-indicted-for-logic-bomb/d/d-id/1076111; Press Release, Dep't of Justice, Former Employee Of Fannie Mae Contractor Convicted Of Attempting To Destroy Fannie Mae Computer Data (Oct. 4, 2010), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2010/makwanaConvict.pdf; Press Release, Dep't of Justice, Fannie Mae Computer Intruder Sentenced To Over 3 Years In Prison For Attempting To Wipe Out Fannie Mae Financial Data (Dec. 17, 2010) ("Malicious Code Would Have Destroyed Mortgage Information"), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2010/makwanaSent.pdf.
- *United States v. Douglas James Duchak*, (D. Colo. 2010) (No. 10-CR-131-MSK): The defendant was convicted by plea agreement of violating one count of 18 U.S.C. §§ 1030(a)(5)(A), 1030(b), and 1030(c)(4)(B). He was a data analyst working as a government contractor at the Transportation Security Administration and had first been told that his responsibilities were being transferred to another employee, and later that his position was being eliminated and his employment terminated. He deleted instructional code from an arrest warrant database and inputted code to replace it, on a designated date, in the Terrorist Screening database. He was sentenced to 24 months in prison. *See* Kim Zetter, *TSA Worker Gets 2 Years for Planting Logic*

Bomb in Screening System, WIRED (Jan. 12, 2011), *available at* http://www.wired.com/threatlevel/2011/01/tsa-worker-malware; Press Release, Dep't of Justice, Colorado Springs Man Indicted For Attempting To Corrupt TSA Computer Database (Mar. 10, 2010), *available at* http://www.justice.gov/usao/co/news/2010/March10/3_10_10.html.

- *United States v. Yung-Hsun Lin*, (D.N.J. 2007) (No. 06-CR-00963-JLL): The defendant, a former computer systems administrator for Medco Health Solutions, Inc., was convicted by plea agreement for planting a "logic bomb" on company computer systems that was designed to "detonate" on his birthday and delete data stored on more than 70 servers, in violation of 18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(c)(4)(A), 1030(b). He was sentenced to serve 30 months in prison. *See* Jaikumar Vijayan, *Unix admin pleads guilty to planting logic bomb at Medco Health, Malicious code would have wiped out critical data on 70 servers*, COMPUTERWORLD (Sept. 21, 2007), *available at* http://www.computerworld.com/s/article/print/9038218/Unix_admin_pleads_guilty_to_planting_logic_bomb_at_Medco_Health; Sharon Gaudin, *Medco sys admin gets 30 months for planting logic bomb, Inside saboteur could have crippled pharmacists' ability to check for deadly drug interactions, U.S. attorney says*, COMPUTERWORLD (Jan. 8, 2008), *available at* http://www.computerworld.com/s/article/9056284/Medco_sys_admin_gets_30_months_for_planting_logic_bomb?intsrc=news_ts_head; Press Release, Dep't of Justice, Former Systems Administrator Admits Planting "Logic Bomb" in Company Computers (Sept. 19, 2007), *available at* http://www.justice.gov/usao/nj/Press/files/pdffiles/Older/lin0919rel.pdf; Press Release, Dep't of Justice, Former Systems Administrator Gets 30 Months in Prison for Planting "Logic Bomb" in Company Computers (Jan. 8, 2008), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2008/linSent.pdf.
- *United States v. William Carl Shea*, (N.D. Cal. 2005) (No. CR 03-20057-RMW): The defendant, who served as the system administrator, planted a "time bomb" on the company network after becoming disgruntled at work. He was convicted in a jury trial for violating 18 U.S.C. § 1030(a)(5)(A)(i). He was sentenced to one year and a day in prison. His conviction was affirmed on appeal. *See United States v. Shea*, 493 F.3d 1110 (9th Cir. 2007). *See also* Press Release, Dep't of Justice, Federal Jury Convicts Former Technology Manager Of Computer Hacking Offense Defendant Found Guilty of Placing Computer "Time Bomb" On Employer's Network Following Employment Dispute (Sept. 8, 2005), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2005/sheaConvict.htm; Press Release, Dep't of Justice, Former Technology Manager Sentenced To A Year In Prison For Computer Hacking Offense (June 23, 2006), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2006/sheaSent.htm; *San Jose man sent to prison for computer 'time bomb,'* SILICON VALLEY BUSINESS JOURNAL (June 23, 2006) ("The malicious code was written to delete the source code but officials eventually found a copy on a backup tape, investigators said."), http://www.bizjournals.com/sanjose/stories/2006/06/19/daily78.html.
- *United States v. Roger Duronio*, (D.N.J. 2006) (No. 02-CR-00933-JLL): The defendant, the former systems administrator at UBS Paine Webber, was convicted at trial on one count of securities fraud and one count of computer fraud in violation of 18 U.S.C. § 1030(a)(5)(A)(i), 1030(c)(4)(A); the jury acquitted on two mail fraud counts. A logic bomb, planted by the defendant after he received a lower bonus than he thought he should have received, damaged more than 1,000 UBS Paine Webber computer stations. The securities fraud conviction was based on his purchase of "put options" after he anticipated the company stock would decrease upon news of the computer logic bomb. He was sentenced to 97 months in prison. *See United States v. Duronio*, 2006 WL 1457936, at *4 (D.N.J. May 23, 2006) (denying motion to dismiss indictment); *United States v. Duronio*, 2006 WL 3591259, at *1 (D.N.J. Dec. 11, 2006) (denying motion for a new trial). The conviction and sentence were affirmed on appeal. *See United State v. Duronio*, 2009 WL 294377 (3d Cir. Feb. 9, 2009). *See also* Sharon Gaudin, *Ex-UBS Systems*

Admin Sentenced To 97 Months In Jail, INFO. WEEK (Dec. 13, 2006) ("Roger Duronio was found guilty of computer sabotage and securities fraud for writing, planting, and disseminating malicious code that took down up to 2,000 servers."), http://www.in formationweek.com/ex-ubs-systems-admin-sentenced-to-97-months-in-jail/d/d-id/1049873; Press Release, Dep't of Justice, Disgruntled UBS PaineWebber Employee Charged with Allegedly Unleashing "Logic Bomb" on Company Computers (Dec. 17, 2002), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2002/duronioIndict.htm.

- *United States v. Timothy Lloyd*, (D.N.J. 2002) (No. 98−CR−00061−WHW): The defendant, a former computer network administrator at Omega Engineering Corp., was convicted at trial for violating of 18 U.S.C. §§ 1030(a)(5)(A). The time bomb deleted about 1,200 computer programs. He was sentenced to 41 months in prison and his conviction was affirmed on appeal. *See United States v. Lloyd*, 269 F.3d 228 (3d Cir. 2001) (reversing grant of new trial and reinstating conviction). *See also* Press Release, Dep't of Justice Press, Former Computer Network Administrator at New Jersey High-Tech Firm Sentenced to 41 Months for Unleashing $10 Million Computer "Time Bomb" (Feb. 26, 2002), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2002/lloydSent.htm.
- *United States v. John Michael Sullivan*, (W.D.N.C. 2000) (No. 99−CR−00122−RLV): After the defendant, a computer programmer, became upset at work, he planted a "logic bomb" into the company's software, which disabled 824 hand-held computers used by company sales representatives. A jury convicted him of violating 18 U.S.C. § 1030(a)(5)(A). He was sentenced to serve 24 months. His conviction and sentencing were affirmed on appeal. *See United States v. Sullivan*, 40 F. App'x. 740 (4th Cir. 2002) (per curiam). *See also* Timothy Roberts, *FBI targets computer crime*, CHARLOTTE BUS. Journal (June 19, 2000), *available at* http://www.bizjournals.com/charlotte/stories/2000/06/19/focus1.html?page=all.

XI. Conclusion

A time bomb case is a distinct form of computer intrusion, often designed to cause significant harm by destroying particular company records. Investigating and prosecuting time bomb cases presents some unique issues and challenges. As the past cases have shown, most often the time bomb is planted by a disgruntled insider who exploits specific vulnerabilities on the company network. The defendant may have unique familiarity with the company network and computer records that are targeted for destruction. There may be labor dispute issues that provided the motive to plan and execute the time bomb. Much of the evidence will be electronic. The time bomb may have been designed to launch when the defendant has an alibi or no longer has access to the company network.

Based on past cases, a five-part process—focusing on the operation, access, ability, knowledge, and motive—may help identify those responsible for the time bomb. This process, in conjunction with other steps, may help identify the most useful evidence and new leads, and focus the presentation of evidence at trial. These steps may aid the jury in understanding how the time bomb operated and determining whether the evidence confirms the defendant's role beyond a reasonable doubt.❖

ABOUT THE AUTHOR

❑ **Mark L. Krotoski**, a federal prosecutor since 1995, previously served as National Computer Hacking and Intellectual Property (CHIP) Program Coordinator at the Computer Crime and Intellectual Property Section in the Criminal Division for nearly four years, and as a CHIP prosecutor in the Northern and Eastern Districts of California for about eight years, among other positions. He has handled a variety of computer intrusion and time bomb investigations and cases including the jury trial conviction in *United States v. Shea*, 493 F.3d 1110 (9th Cir. 2007). ✠

The views expressed in this article do not necessarily reflect those of the United States Department of Justice.

From the P.R.C. to the F.C.I.—Cracking a Chinese Cybercrime Case

Edward J. McAndrew
Assistant United States Attorney
District of Delaware

On June 6, 2011, Xiang Li arrived on the Island of Saipan from his home in Chengdu, China, a city located in the southwestern Sichuan Province. He traveled there to deliver 20 gigabytes of highly sensitive data exfiltrated from a cleared defense contractor, along with over $1 million in cracked, industrial-grade software used in U.S. military, intelligence, and other sectors. Li, a member of a loose confederation of intellectual property thieves, thought he was meeting two Americans who had purchased this intellectual property from him and were interested in helping him sell similar items in the United States. Instead, he was meeting a team of Homeland Security Investigations agents who had been tracking his actions and cultivating an online relationship with him for 18 months. At the end of a recorded undercover meeting in a Saipan hotel, Li was arrested and flown to Wilmington, Delaware, where he would be sentenced to 12 years in federal prison. By the time he was taken into custody, Li and others associated with him had used the Internet to steal and crack over $100 million worth of sensitive software from over 200 technology companies and to disseminate that software to over 400 customers located in 28 states and 60 foreign countries.

This article will share insights into the investigation and prosecution of Li and some of his well-placed U.S. customers. It will discuss how we addressed some of the key issues that arose during the cases against Li and his customers—from initial attribution, through charging, takedown, prosecution, and sentencing. Finally, this article will offer tips on working with organizational victims in international cyber-theft cases.

I. A cybercrime investigation resulting from a victim disclosure

The investigation began with agency outreach and a victim-company report. As part of its counter-proliferation strategy and Export Enforcement Program, U.S. Customs and Immigration Enforcement, Homeland Security Investigations (HSI) conducts industry outreach through "Project Shield America." Through meetings and presentations, HSI seeks to "protect the technical accomplishments resulting from American ingenuity and labor" and to "prevent[ ] our adversaries from achieving

technological parity or gaining a military advantage through illegal acquisition of U.S. technology." ICE, PROJECT SHIELD AMERICA FACT SHEET, *available at* http://www.ice.gov/project-shield/.

In December 2009, HSI agents conducted an outreach meeting with representatives of a "cleared defense contractor" (CDC) that produces export-controlled simulation software used in military, intelligence, space, and aerospace applications. (A CDC is "a private entity granted clearance by the Department of Defense to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of the Department of Defense." *See* National Defense Authorization Act for Fiscal Year 2013, H.R. 4310, P.L. 112-239, § 941(e)(1).) During that meeting, the company's export control officer notified the agents about a China-based Web site that was advertising the company's signature software product for sale. The company never authorized the Web site operators to sell the product and did no business in China. The company also did not know how the Web site operators were obtaining its tightly controlled software and disabling its electronic access and copy control features before disseminating it online. Because this was a mid-sized company built around this one suite of highly valuable and export-controlled software, the unfettered release of that software online created enormous financial, reputational, and regulatory risks for the company.

A. Early investigation and attribution efforts

Following the victim-company's notification, HSI launched an investigation into the Web site and into how those behind it were obtaining, modifying, and selling sensitive software from China. The investigation began with a full review and documentation (through Camtasia recordings and screen captures) of the Web site. The review revealed that the Web site, located at www.crack99.com, was advertising over 2,000 industrial-grade software products used in numerous applications, including aerospace simulation and design, defense, electronics, energy, engineering, explosive simulation, intelligence gathering, manufacturing, mining, space exploration, mathematics, storm water management, and manufacturing plant design. Most of these products were export controlled and were generally sold to government contractors, governmental entities, universities, or companies engaged in the research and development of components or products throughout the supply chain.

The Web site claimed that all of the advertised software was pirated or "cracked," meaning that the software's licensing system files and other access and copy control features had been disabled. As a result of the cracking, anyone in possession of the software would have the ability to access and copy it. The Web site offered the software for pennies on the dollar in most cases.

Unlike other software piracy Web sites we had investigated, the Crack99 Web site was relatively crude. The text was written in broken English, with Chinese characters interspersed. It linked to similar Web sites, some of which were entirely in Chinese text. It had no linked electronic payment processing mechanism, and therefore really served only as an advertising site. It listed payment methods including wire transfers through Western Union, Money Gram, WebMoney Transfer, and E-Gold. It included one gmail address to which purchase inquiries were to be sent.

We began the attribution process with open source research, grand jury subpoenas, and pen trap and trace orders. We obtained subscriber records and logs for the gmail address through subpoena. We caught a very big, early break when the subscriber records for that gmail account included a subscriber name ("lixiang li"), logs, a secondary Yahoo address, and a list of Google services used by the account holder, including Google Docs, Search History, Transliteration, Webmaster Tools, and Analytics. Subsequent analysis of that data provided strong corroboration of the account user's identity.

We also ran trace routes on all the linked Web sites and then issued subpoenas to delineate domain registration activity and Web site hosting services and locations. Responsive records included over 1,800 domain registrations in the name of "Xiang Li" of Chengdu, China. The National Cyber-Forensics & Training Alliance (NCFTA) provided a tremendously helpful analysis of related IP addresses, domain registration information, Web sites, email accounts, and complaints received by the

Internet Crime Complaint Center. The NCFTA is a non-profit organization based in Pittsburgh that provides

> a neutral collaborative venue where global partners from industry, law enforcement and academia come together, leveraging cross-sector resources to more effectively analyze critical, real-time intelligence against emerging cyber threats. The actionable intelligence developed is used to mitigate and ultimately neutralize persistent global cyber threats, in an effort to protect intellectual assets, countries and citizens.

NCFTA MISSION STATEMENT, *available at* http://www.ncfta.net/. The NCFTA has formal partnership agreements with more than 40 U.S. private sector organizations and more than 15 U.S. and international law enforcement or regulatory agencies. Both HSI and the FBI have points of contact embedded at the NCFTA to provide case support to the field. In this case, NCFTA's investigative work yielded a detailed map of the infrastructure being used to distribute the stolen intellectual property, including a list of hosting services in the United States that would be targets for search and seizure.

B. Controlled purchases and email search warrants

In January 2010, HSI agents made their first controlled purchase from the Crack99 Web site. The agents sent an email to the gmail account listed on the Web site and inquired about purchasing a program called "Satellite Toolkit." That software is used for aircraft and unmanned aerial vehicle (UAV) systems, communications and electronic warfare, geospatial intelligence, missile defense, navigation, range safety, space exploration, space superiority, and spacecraft mission design and operations. Not unlike much of the other software at issue in the case, "Satellite Toolkit" was designed and manufactured by a 250-employee company located in the United States. Certain modules within this software suite are controlled by the Department of Commerce's Export Administration Regulations or the Department of State's International Traffic in Arms Regulations.

The agents then began an email-based dialogue with the gmail account user who referred to himself as "Xiang Li" and offered to sell them a cracked version of "Satellite Toolkit" for $1,000. Xiang Li also provided another name and address to which a Western Union payment could be sent. Days after the agents wired payment to China, they received an email from "Xiang Li" providing hyperlinks to a U.S. server from which they downloaded three .rar files that contained the "Satellite Toolkit" software and a cracked license file needed to access it. The victim-company subsequently examined the software, confirmed its authenticity, and analyzed the manner in which the access and copy controls had been disabled through the "cracked" license file.

Based on the information developed through the first controlled purchase, we obtained a search warrant for the gmail account used by Xiang Li during the transaction. Over the next 15 months, we executed 3 additional search warrants on that account. In total, we obtained over 25,000 emails from the account, most of which were related to over 700 transactions in cracked, sensitive software. The emails also revealed that Xiang Li's role extended beyond the negotiation of price, collection of money, and dissemination of download links to the software. Because of the complexity of the software, Xiang Li would remain intensely involved in the customer's installation and use of the software, serving a customer support role that was essential to even the engineers, scientists, and other sophisticated purchasers of the software.

The analysis of the tens of thousands of emails in this single gmail account led to the identification of over 400 customers of the Crack99 Web site operation. HSI agents then executed search warrants on numerous other email accounts that had significant contact with Xiang Li's gmail account. The results of those search warrants were used to identify the account users, more than two-thirds of whom were Americans. Subpoenas relating to those individuals' financial accounts were used to confirm purchases of contraband software from Crack99 and other criminal outlets. In total, we collected and

reviewed over 75,000 email messages that related to the purchase and installation of stolen software through the Crack99 Web site or other sources.

Between January 2010 and June 2011, HSI agents conducted a series of additional controlled purchases of cracked software advertised on the Crack99 Web site, each time having extensive online communications with Xiang Li. The agents corresponded by email with Li about their purchases, including negotiating price, receiving electronic files containing the pirated software or hyperlinks that enabled agents to download the pirated software from computer servers located in the United States, and receiving instructions from Li on how to install the pirated software. In addition to purchasing other versions and modules of "Satellite Toolkit," the agents also purchased industrial-grade and export controlled software used for aerospace simulation and design, explosive simulation, manufacturing, electronics, plant design, energy generation and transmission, and automotive, biomedical, defense equipment, and weapon design. In total, the agents transmitted $8,615 to Xiang Li and a coconspirator and received over $1 million worth of software.

C. Developing an online relationship and opportunities to capture the target

Over an 18-month period, HSI agents developed an ongoing dialogue with Xiang Li that provided various clues about his interests and motivations. They also progressed beyond email to Skype calls and instant message conversations with Li. They learned, for instance, that Li was part of a loose confederation of hackers and crackers that stole mostly American technology, disabled its access and copy controls, and distributed it online. This confederation was able to obtain access not only to tightly controlled software, but also to internal data about that software from its manufacturers. Xiang Li was one of the middlemen in this confederation, who was responsible for disseminating the software and assisting customers in the complicated and often laborious process of installing and operating it. They also learned that Li and others were interested in enhancing their U.S.-based storage and distribution architecture. Finally, and perhaps most importantly, they learned that Li was a frustrated graphic artist who had a strong interest in producing software complete with counterfeit labeling and packaging.

Using what they learned through their extensive communications with him, the HSI agents convinced Li that they were interested in establishing a partnership with him and his colleagues, whereby the agents could serve as a U.S.-based reseller of cracked software at higher prices. Playing on Li's interest in counterfeiting, the agents convinced him that they could make large amounts of money by selling cracked software on disks with counterfeit labeling and packaging in the United States.

We had successfully developed a strong relationship with a cybercriminal located in China. In November 2010, we obtained a sealed indictment against Li and a coconspirator. The United States, however, has no extradition treaty with China. As the agents went about strengthening their relationship with Li and selling him on the idea of their joining the criminal enterprise, we evaluated options for arresting Li and his coconspirator outside of China.

The options for obtaining custody of them included arresting them in the United States or a U.S. territory, or requesting their provisional arrest in a country that might be amenable to extraditing them to the United States. *See* DEP'T OF JUSTICE, U.S. ATTORNEYS' MANUAL § 9-15.230 (2014). We based our indictment on the undercover purchases we had made to that point and transactions we could establish through email and financial records. We fully expected to supersede the indictment if we proved successful in arresting them or, before the filing of an extradition request, if another country was able to provisionally arrest them outside of China.

We then turned our attention to attempting to "lure" Li and his coconspirator out of China to somewhere we or a cooperative foreign law enforcement agency could arrest them. A "lure" is

> a subterfuge to entice a criminal defendant to leave a foreign country so that he or she can be arrested in the United States, in international waters or airspace, or in a third country

> for subsequent extradition, expulsion, or deportation to the United States. Lures can be complicated schemes or they can be as simple as inviting a fugitive by telephone to a party in the United States.

Id. § 9-15.630. Because of the sensitivity associated with lures, "a prosecutor must consult with the Office of International Affairs before undertaking a lure to the United States or a third country." *Id.*

We began coordinating with the Office of International Affairs (OIA) and various ICE attaché offices on possible lure sites soon after obtaining our indictment. Because of the evolving investigation and uncertainty surrounding whether, and to where, Li or his coconspirator would travel, we spent about eight months raising and evaluating (and ultimately rejecting) various possible lure sites. This was a time-consuming process that involved much communication with various entities both here and abroad. Prosecutors who are contemplating such operations should involve OIA and attaché offices as early as possible in the planning process and plan for a long haul.

On the investigative end, our agents told Li that they were planning on traveling to areas around Southeast Asia in the spring or summer of 2011. In particular, the agents told Li they would be in the Philippines during their travels, which we believed could be a viable option for Li's arrest and extradition to the United States. During the same time period, Li had offered to sell the agents internal data from a cleared defense contractor that related to one of the software products they had purchased. In a stroke of luck, and because he evidently did not fear U.S. prosecution or understand international fugitive operations, Li offered to meet the agents in Saipan to deliver the internal data and cracked software with counterfeit labeling and packaging that he had designed. Li expressed his hope that the agents would find the counterfeit items to be of acceptable quality, in which case he would produce more for resale in the United States.

D. The undercover meeting/arrest and digital infrastructure takedown

Meeting and arrest in Saipan: On June 6, 2011, Li flew from China to Saipan to meet with the undercover agents. Armed with a picture that Li had sent them, HSI agents confirmed Li's arrival as he walked off the plane in Saipan. A team of agents then maintained surveillance on him until the next day, when he arrived at a hotel for his scheduled meeting with them.

Prior to the meeting, the agents had equipped the room with recording devices that would capture video and audio of Li delivering the counterfeit software products and 20 gigabytes of confidential data exfiltrated from an internal server of a cleared defense contractor. The undercover agents also planned to engage Li in a conversation in which he would likely make various incriminating statements.

The meeting went as planned, with Li handing the agents the contraband in perfect view of the camera. During the recorded conversation, Li erased any doubt that he knew he was violating U.S. intellectual property laws by selling the pirated software and counterfeit labeling and packaging. Li's demeanor and tone during the meeting illustrated an attitude of complete disregard for American law and for the rights of the victim-companies—powerful visual evidence for any trial and sentencing. For example, Li told the agents that he received various "cease and desist" demands via email from software manufacturers, but he would simply delete them.

At the conclusion of the meeting, Li was arrested and the items that he brought to the meeting were seized. During a subsequent search of Li's room at another hotel, agents seized various computers and external storage devices. After initial proceedings in the District of the Northern Mariana Islands, Li was flown from Saipan to the District of Delaware for prosecution.

Takedown of the digital infrastructure used to store and distribute stolen software: As soon as Li was in custody in Saipan, we immediately dismantled all parts of the storage and distribution infrastructure within our jurisdictional reach. Our objectives in doing so were to stop others associated

with Li from continuing to operate the Crack99 and related Web sites or to otherwise distribute cracked software. To mitigate the damage to the victim-companies, we also wanted to recover as much of the contraband software and other intellectual property as possible. Finally, of course, anything seized could be useful at trial or sentencing.

To complete the takedown, HSI agents executed search and seizure warrants on all U.S.-based servers linked to Li. This simply required the Web hosting companies to disable and copy the drives that contained data associated with the Web sites. These warrants were sworn out before a magistrate in Delaware, pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A), and Federal Rule of Criminal Procedure 41(e)(2)(B).

HSI agents also executed seizure warrants on the domain names registered to Li and used in the commission of the crimes. Forfeiture of the domain names was authorized under 18 U.S.C. § 2323, which provides for civil and criminal forfeiture of "[a]ny property used, or intended to be used, in any manner or part to commit or facilitate the commission of [violations of §§ 2318, 2319, 2319A, 2319B, or 2320]." 18 U.S.C. § 2323(a)(1) (2014). Section 2323 further specifies that seizure and forfeiture is governed by 21 U.S.C. § 853, which provides that "[t]he Government may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant." 21 U.S.C. § 853(f) (2014). Section 853(l) authorizes federal courts to enter orders regarding criminal forfeiture without regard to the location of any property that may be subject to forfeiture. *See id.* § 853(l); *see also* 18 U.S.C. § 981(b)(1) (2014) (authorizing Attorney General to seize property subject to forfeiture to the United States) and § 981(b)(3) ("[A] seizure warrant may be issued . . . by a judicial officer in any district in which a forfeiture action against the property may be filed. . . and may be executed in any district in which the property is found . . . .").

To effectuate the seizures, VeriSign, Inc., as the registry for the ".net" and ".com" top-level domains, was directed to restrain and lock the domain names pending transfer of all right, title, and interest in them to the United States upon completion of forfeiture proceedings. VeriSign was further directed to delete all information from the records relating to the owner of the domain names, pending the completion of forfeiture proceedings. VeriSign also was directed to disable the DNS resolution of the domain names by changing or deleting any records, databases, tables, or documents that are used to enable domain name resolution for the domain names. After these steps were taken, queries to the domain name service for the domain names returned nothing or a "host not found" error message.

Upon completion of forfeiture proceedings, VeriSign would be directed to configure the DNS resolution of the domain names to an Internet Protocol Address to be provided by HSI, and at which HSI would display a webpage with a forfeiture notice. All domain name records also would be updated to reflect the transfer of ownership to the United States.

Forensic analysis of seized equipment: Upon return to Delaware, HSI conducted forensic analyses of the computer equipment and removable digital media seized from Li for use in his or any related trial and sentencing. The analyses confirmed that the equipment contained pirated copies of the software ordered by the undercover agents and counterfeit packaging and documentation for such software. The equipment also contained scores of other cracked software programs, installation and operational data relating to the programs, data files associated with the operation of the Crack99.com and related Web sites, and communications between Li and his coconspirators.

Copies of particular cracked software and related data found on the computer equipment were provided to those victim-companies that were willing to analyze the material. This was done for a number of reasons. First, the companies' analyses could assist in our prosecutions. Second, providing the data might assist the companies in determining how their products were being stolen and cracked, allowing them to take remedial measures. Third, they could use the data to make any required disclosures to the Departments of Defense, State, and Commerce, or other government agencies or affected parties.

Involving the victim-companies in the forensic analysis of "their data" is a critical step in these investigations. They know much more about their product and data than we do. They can identify that which we may miss, and they can help us understand and articulate the full scope and negative impact of the crime. Some companies were extremely appreciative and motivated to assist in the prosecution. For example, one CDC confirmed that Li had delivered 6 disks containing approximately 20 gigabytes of proprietary data exfiltrated from the company's internal file transfer protocol server. This data related to the software license server; training and "flash videos" used to teach users how to operate the software; mapping data files including three-dimensional imagery files; military and civilian aircraft image models; a software module containing data associated with the International Space Station; a complete listing of all of the software modules created by the company and the three-dimensional graphic images associated with these modules; various programmer training courses; other files including PDF and power point files associated with the software; and a high resolution, three-dimensional imaging program. The disks even contained music files uploaded by the company's employees to the internal server and then stolen by hackers. This was dynamite evidence to have available for trial and sentencing.

II. Insight into an international cybercrime group

Xiang Li began actively cooperating with HSI agents upon his arrest. Over multiple debriefings that included online activities, Li provided valuable insight into the workings of cybercrime groups focused on the cyber-theft and cracking of software related to defense and intelligence technology. At least insofar as Li revealed, these "groups" are more accurately described as loose confederations of hackers and crackers, as opposed to highly structured organizations. Below are some of the details that we learned from Li and corroborated through other evidence.

Li provided information and online illustrations of some of the methods that China-based cybercriminals employ to obtain, crack, and distribute software via the Internet. First, they obtain legitimate copies of the software by a variety of means, including: (1) hacking or otherwise using unauthorized access into private computer networks, (2) free software demonstration or trial copies (which limit modules or duration of access through license files), (3) Web site downloads, (4) unauthorized release of beta versions of software, (5) rogue employees providing the software to them, and (6) unscrupulous foreign distributors of the software.

Second, software "crackers" loosely organize into "Fan Groups" and crack software by disabling the access and copy controls. These groups usually specialize in cracking certain types of software. The "Fan Groups," which operate mostly in China and Russia, make the cracked software available on Web sites, forums, and other online portals based in China. These Web sites, forums, and portals often specialize in specific types of technology or industry sectors. For instance, Li showed the agents a number of forums focused specifically on software related to defense technology, including forums offering ITAR-controlled software modules for sale.

Third, other cybercriminals obtain the cracked software from forums, Web sites, file transfer protocol sites, or other means. They also may purchase the software directly from hackers who find particular versions of software that are not otherwise available. These "middle men" operate Web sites that advertise cracked software products and distribute it to illicit customers around the globe. A portion of their sales price is paid to the hackers and crackers who procure and crack the software. The "middle men" generally specialize in, and guide customers through, the complex technical installation process. Without these "middle men," stolen industrial-grade software is often inoperable and non-transferable.

III. Charging decisions

A. Possible substantive charges in intellectual property cyber-theft cases

In April 2012, a grand jury returned a superseding indictment charging Li and a coconspirator with a variety of intellectual property and related offenses. For various practical reasons, we chose not to add some available charges. Below is a summary of potential charges that prosecutors may consider under facts similar to those described in this article.

The first group of potential charges is composed of particular intellectual property crimes and conspiracies to commit them. Li and his coconspirator were charged with each of these violations. A principal charge under facts similar to those at issue in Crack99 is criminal copyright infringement and conspiracy to commit it, based on the unauthorized reproduction and dissemination of copyrighted software. *See* 17 U.S.C. § 506 (2014); 18 U.S.C. §§ 371 & 2319(a), (b)(1) (2014). Where software license files have been cracked to enable access and copying of software, prosecutors also should consider charging defendants with circumvention of access and copy controls (and conspiracy), in violation of the Digital Millennium Copyright Act (DMCA). *See* 17 U.S.C. §§ 1201(a)(1), 1204 (2014); 18 U.S.C. § 371; *see also Murphy v. Millennium Radio Grp. LLC*, 650 F.3d 295, 300 (3d Cir. 2011). By obtaining the cracked license files from others and then transmitting them to others, Li and his coconspirator also violated the anti-trafficking provision of the DMCA. *See* 17 U.S.C. §§ 1201(a)(2), 1204; 18 U.S.C. § 371; *see also Tracfone Wireless, Inc. v. Anadisk LLC*, 685 F. Supp. 2d 1304, 1316–17 (S.D. Fla. 2010). We also charged the defendants with trafficking in counterfeit labels, documentation, and packaging as to the items Li brought to the Saipan meeting. *See* 18 U.S.C. § 2318(a) (2014).

A second group of charges can be found in the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and similar network crimes statutes. *See* COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, CRIMINAL DIV., DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 12-34, 96-104 (Scott Eltringham, 2d ed. Nov. 2010) (providing an overview of those crimes). Due to victim concerns with proving unauthorized access to sensitive networks, and because of the overwhelming evidence we had to support various other charges, we chose not to include a § 1030 count in the Crack99 indictment.

The next group of charges that may be considered in cases of this type includes more traditional fraud and theft statutes. For instance, wire fraud is a common and powerful charge that can be included in many cybercrime cases. *See* 18 U.S.C. § 1343 (2014). The penalties for wire fraud (maximum of 20 years imprisonment), for instance, are much more significant than those for most unauthorized access violations under § 1030 or copyright violations under § 2319. Wire fraud, however, should not be viewed "as a substitute for a copyright charge in the absence of evidence of any misrepresentation or scheme to defraud." COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, CRIMINAL DIV., DEP'T OF JUSTICE, PROSECUTING INTELLECTUAL PROPERTY CRIMES 73 (Kathleen Baker, 3d ed. 2006) (citing *United States v. LaMacchia*, 871 F. Supp. 535, 540 (D. Mass. 1994)). *But see United States v. Manzer*, 69 F.3d 222, 226 (8th Cir. 1995) (affirming wire fraud conviction for sale of cable television descrambling equipment); *United States v. Coyle*, 943 F.2d 424, 427 (4th Cir. 1991) (similar). In the Crack99 case, we included wire fraud and related conspiracy counts. Our theory was that the defendants obtained software from others who had misrepresented their intent to secure trial licenses to the software or who had hacked into computer networks to obtain confidential data or software. We also had numerous emails from Li to victim-companies falsely promising to cease and desist unauthorized distribution of their software. Finally, after installation by Crack99's customers, many of the software and cracked licensing files would communicate with access control and other servers operated by the victim-companies or their agents/vendors, essentially misrepresenting their authorization to do so.

Charging a violation of the National Stolen Property Act may be considered if "goods, wares, [or] merchandise" that have been stolen or taken by fraud are "transport[ed], transmit[ted], or transfer[red] in interstate or foreign commerce." 18 U.S.C. § 2314 (2014). Courts have interpreted this statute to apply

only to "tangible" items though. *See, e.g.*, *Dowling v. United States*, 473 U.S. 207, 216 (1985). *Compare United States v. Agrawal*, 726 F.3d 235, 251–53 (2d Cir. 2013) (affirming NTSA conviction where defendant printed source code on paper he stole from employer), *with United States v. Aleynikov*, 676 F.3d 71, 76–78 (2d Cir. 2012) (reversing NTSA conviction where defendant stole source code from employer by uploading it to server in Germany and then downloading it to computer devices in New Jersey). Although no court seems to have addressed the issue, the same concern may arise with bringing a charge for smuggling of goods, in violation of 18 U.S.C. § 545, for this type of conduct. Like § 2314, § 545 focuses on the unlawful movement of "merchandise" and "goods."

Prosecutors also should consider charging financial crimes where appropriate. Money laundering is a primary charge in many cybercrime cases. Violations of the Computer Fraud and Abuse Act and the criminal intellectual property statutes constitute "specified unlawful activit[ies]" under the money laundering statutes. *See* 18 U.S.C. §§ 1956(a), (c)(7)(D), 1957, 1961(1); *see generally* Jaikumar Ramaswamy et al., *Money Laundering and Forfeiture*, 61 U.S. ATTORNEYS' BULLETIN 1, 1–75 (Sept. 2013), *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab6105.pdf.

Finally, cyber-theft from U.S.-based companies and distribution of sensitive software outside of the United States may violate export control laws. The two primary export control laws that may be implicated are the Arms Export Control Act (AECA) and the International Emergency Economic Powers Act (IEEPA). The AECA and its International Traffic in Arms Regulations (ITAR) proscribe the export of "defense articles, defense services, and related technical data" without first obtaining a license from the Department of State. *See* 22 U.S.C. § 2778(c), (j)(4) (2014); 22 C.F.R. §§ 121.1, 126.1 (2014). The IEEPA is used to enforce the Export Administration Act of 1979 and the Export Administration Regulations, which prohibit the unlawful export of "dual-use" goods and technology. *See* 50 U.S.C. §§ 1702, 1705(b) (2014); 15 C.F.R. §§ 730.3, 774.1 (2014); 31 C.F.R. §§ 542.101–.901, 596.101–.901 (2014). Charging violations of these statutes requires consultation with, and approval of, the National Security Division. *See* DEP'T OF JUSTICE, U.S. ATTORNEYS' MANUAL § 9-90.020 (2014).

We ultimately decided not to include an export control charge in the Crack99 case. Had we done so, our theory would have been that export controlled software created in the United States was transmitted to China without necessary licenses through one of the various methods described in Part II above. Li and others then sold cracked software without export licenses, in some instances to individuals in embargoed countries. In many of these transactions, the controlled software was uploaded from computers in China to servers in the United States, from which Crack99 customers downloaded it to computers located around the world (including in embargoed countries). In a virtual sense, this software left the United States, returned again, and then was unlawfully re-exported.

B. Extradition considerations at the charging stage

Prosecutors also should consider the potential effects of charging decisions on extradition efforts. Two concepts to keep in mind when selecting charges are "dual criminality" and the "rule of specialty." The doctrine of dual criminality provides that criminal conduct may be extraditable only where the conduct is criminal under the laws of both the requested and requesting countries. *See, e.g.*, *Gallo-Chamorro v. United States*, 233 F.3d 1298, 1306 (11th Cir. 2000); *United States v. Herbage*, 850 F.2d 1463, 1465 (11th Cir. 1988); *Quinn v. Robinson*, 783 F.2d 776, 783 (9th Cir. 1986). The crimes need not be identical in both countries. *See, e.g.*, *Collins v. Loisel*, 259 U.S. 309, 312 (1922); *see also* Ryan P. Fayhee, *Extradition in Export Enforcement Cases*, 61 U.S. ATTORNEYS' BULLETIN 1, 1–2 (Nov. 2013), *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab6106.pdf; Glenn W. McTaggart, *A Brief Primer on International Extradition Practice*, 44 U.S. ATTORNEYS' BULLETIN 12, 12–16 (Dec. 1996), *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab4406.pdf. Not all U.S. crimes may satisfy the doctrine. For example, one author recently noted the practice of including wire fraud charges in export control cases where possible, due to the difficulty of extraditing targets based on IEEPA charges. *See* Mark Roomberg, *Challenges and Lessons Learned in IEEPA Counter-Proliferation*

Cases: United States v. Susan Yip, 61 U.S. ATTORNEYS' BULLETIN 37, 39 (Nov. 2013), *available* at http://www.justice.gov/usao/eousa/foia_reading_room/usab6106.pdf. Due to the divergent treatment of computer and intellectual property crimes in different countries, early attention to this concept may be critically important to a successful extradition request.

Prosecutors also should consider, *at the charging stage*, the possible effects of the "rule of specialty" on extradition. In general, the rule of specialty permits a defendant to be prosecuted in the United States only for those crimes for which he has been extradited. *See, e.g.*, *United States v. Stokes*, 726 F.3d 880, 889 (7th Cir. 2013) (collecting cases); *United States v. Lehder-Rivas*, 955 F.3d 1510, 1519–20 (11th Cir. 1992). It is therefore important to include all significant charges in the indictment submitted as part of the extradition request. After extradition, prosecutors may encounter difficulty adding new types of charges or even additional violations of the statutes under which the defendant has been extradited. Prosecutors should contact OIA for assistance in responding to defense motions raising a specialty claim. *See* DEP'T OF JUSTICE, U.S. ATTORNEYS' MANUAL § 9-15.500 (2014).

IV. Spin-off cases against high-value customers of Crack99

Li and his coconspirators engaged in over 700 transactions through which they distributed over $100 million in pirated software to over 400 customers located in 28 states and 60 foreign countries. Much of the stolen software and related technology were industrial-grade, digital engineering tools used to design myriad products essential to daily life, the health and safety of the public, and U.S. national security. Based on information gathered throughout the subpoena and search warrant phases of the investigation, we confirmed that Crack99's customers included foreign governments, employees of the U.S. Government, defense contractors, engineers, small businesses, and individuals located in embargoed countries.

We ultimately were not successful in apprehending any Crack99 customer located in embargoed countries. It is worth noting, though, how the Crack99 operation served as a way for those in embargoed countries to obtain software they could not lawfully purchase. In February 2010, for example, a Syrian national emailed a U.S. software company seeking a quote on an electronic design automation software product valued at approximately $24,000. The U.S. software company informed the Syrian national that U.S. law prohibited it from selling this software to those in Syria. The Syrian national then emailed Li, who sold the cracked software product to the Syrian national for $185. Li provided the Syrian national with hyperlinks to a server located in the United States, from which the customer could download the software. When that failed due to the slow speeds and capacity of the Syrian's Internet service, Li mailed disks containing the software to Syria.

We had much better success going after high-value American customers of Crack99. Prior to the Saipan takedown of Xiang Li, we identified nine, high-value American customers located in six federal districts. We conducted email search warrants on each and confirmed transactions between each target and Crack99. Two of the six districts (the District of Maryland and the Western District of Kentucky) assisted us with searches and were willing to pursue the cases criminally if they could not be resolved in Delaware. Other districts were not responsive to proceeding against customers who purchased a low number of pirated software programs from the Crack99 Web site.

With Li in federal custody, we moved against the targets in Maryland and Kentucky. Both were among Crack99's biggest customers, and both held significant engineering positions and security clearances.

Our Kentucky target, Dr. Wronald Best, was the "Chief Scientist" for a government contractor that services the U.S. and foreign militaries and law enforcement with a variety of products and components relating to radio transmissions, radar usage, microwave technology, and vacuum tubes. Between November 2008 and June 2009, Dr. Best exchanged over 260 emails with Li and obtained 10

pirated software programs with an estimated retail value of $600,000. Dr. Best obtained other cracked software programs worth millions more from Russian cybercriminals.

Searches of Dr. Best's home and offices at the government contractor resulted in the seizure of computers and equipment containing cracked software, related materials, and communications with various cybercriminals located in China and Russia. In addition to obtaining cracked software from these sources, the investigation revealed that Dr. Best misused his position at the government contractor to obtain software from various technology companies (primarily on a trial license), which he then provided to the Chinese and Russian cracking communities. We also found that Dr. Best had been using cracked software obtained from Crack99 to design components used in military helicopters (including Blackhawk helicopters), Patriot missiles, police radars, and breathalyzer equipment used by the many police departments in the United States. In fact, Dr. Best used cracked software obtained from Chinese cybercriminals to design a component used in the weather radar system employed in the "Marine One" Presidential helicopter fleet.

Our Maryland target, Cosburn Wedderburn, was a NASA electronics engineer working at the Goddard Space Flight Center in Greenbelt, Maryland. Between September 2008 and November 2010, Wedderburn corresponded extensively with Li and purchased 12 cracked software programs with an estimated retail value exceeding $1.2 million. This software had a broad range of applications, including electric engineering, aerospace, telecommunications design, and electronic design automation. Wedderburn used the cracked software for side consulting jobs involving electronic and aerospace simulations, including conducting a thermal simulation contract for China-based Huawei Technologies, Ltd. Wedderburn also uploaded the cracked software he purchased from Li onto a NASA computer network.

V. Convictions and sentencing issues

In March 2012, Best and Wedderburn both pled guilty to conspiracy to commit copyright infringement. Both agreed to testify against Xiang Li if he proceeded to trial. In January 2013, three months before he was scheduled to proceed to trial, Li pled guilty to conspiracy to commit criminal copyright infringement and wire fraud. Requiring Li to plead guilty to the wire fraud conspiracy was critically important to us. The statutory maximum sentence for criminal copyright infringement and conspiracy to commit criminal copyright infringement is five years. 18 U.S.C. §§ 371, 2319 (2014). Li's advisory U.S. Sentencing Guidelines (U.S.S.G.) range greatly exceeded five years because the "infringement amount" or "loss" was over $100 million. *See* U.S. SENTENCING GUIDELINES MANUAL §§ 2B1.1, 2B5.3 (2012). We therefore needed the statutory maximum of 20 years applicable to wire fraud conspiracies to obtain the type of sentence we believed was appropriate. *See* 18 U.S.C. §§ 1343, 1349 (2014).

On June 11, 2013, just days after the world first heard the name "Edward Snowden," and a U.S.-China presidential summit was held in California, Li was sentenced to 12 years in federal prison. Dr. Best was sentenced to one year and one day in prison, as well as three years of supervised release and a $6,000 fine (the amount he paid to cybercriminals for over $2.3 million in cracked software). He also was fired, and his security clearance was revoked. His erstwhile employer was left to respond to inquiries from the Defense Contract Management Agency. Cosburn Wedderburn was sentenced to one year of probation. He too was fired, had his security clearance revoked, and was debarred from government contracting.

We faced two major issues at sentencing in the Li and Best cases. First, the defense in both cases fought to avoid the use of the retail value of the stolen software to calculate the "infringement amount" or "loss" that was key to establishing a high advisory Guidelines range. Second, the defense in both cases argued that imposing significant jail sentences would be unfair. Best's counsel used IP crime sentencing statistics to argue that "these cases are rarely prosecuted" and any jail time is unusual. Li's counsel argued that Li was the product of a culture that did not view the cyber-theft of American technology as criminal.

Defense counsel contended that Li was essentially tricked into leaving China and then hauled halfway around the world and imprisoned for conduct that would not result in a criminal conviction, let alone a prison sentence, in China.

A. Calculating pecuniary harm to victims of digital intellectual property theft

Defendants often argue that the Guidelines calculations for intellectual property crimes should only reflect their actual gain, because the victims suffered no lost sales. Defendants similarly argue for downward variances even if they lose the Guidelines calculation argument.

Li and Best both argued that the victim-companies lost no sales because Crack99's customers would not have purchased the software legitimately. Where particularly sensitive, specialized, and high-value software is at issue, there is only a limited pool of legitimate, available buyers. Because cyber-thieves are not legitimate market participants, the defense theory goes, their stealing such software and providing it to others for unlimited distribution online really does not alter the legitimate market. Thus, they claim, rampant cyber-theft and software piracy is akin to a "no loss" fraud that does not warrant a significant sentence.

This argument should fail under the express language of the U.S. Sentencing Guidelines Manual. The sections applicable to wire fraud and criminal copyright infringement both set relatively low base offense levels and then enhance that level based on the "loss" table contained in § 2B1.1. *See* U.S. SENTENCING GUIDELINES MANUAL §§ 2B1.1(b), 2B5.3(b)(1) (2012). Section 2B5.3(b), which applies to criminal copyright violations, uses the term "infringement amount" to refer to the value of the stolen software. Section 2B1.1(b), which applies to fraud and other economic crimes, uses the term "loss" to refer to the pecuniary harm suffered by victims.

Using the retail value of stolen intellectual property is generally the correct approach for a court to take in calculating the "infringement amount." As explained in Application Note 2(A) to § 2B5.3:

> The infringement amount is the retail value of the infringed item, multiplied by the number of infringing items, in a case involving any of the following:
>
> (i) The infringing item (I) is, or appears to a reasonably informed purchaser to be, identical or substantially equivalent to the infringed item; or (II) is a digital or electronic reproduction of the infringed item;
>
> . . . .
>
> (iii) The retail value of the infringing item is difficult or impossible to determine without unduly complicating or prolonging the sentencing proceeding;
>
> . . . .
>
> (v) the retail value of the infringed item provides a more accurate assessment of the pecuniary harm to the copyright or trademark owner than does the retail value of the infringing item.

Id. § 2B5.3 cmt. n.2(A).

Although the application of any one of these subsections is sufficient, each will independently support use of the retail value of the "infringed item" in most cases. Subsection (i) generally will apply because the pirated software is a digital and electronic reproduction of the copyrighted software. Undercover purchases sent to victim companies for authentication will likely establish this fact. Subsection (iii) generally will apply in large cyber-theft cases because proving the retail value of a large

number of products owned by a large number of manufacturers will often substantially prolong a sentencing hearing. Subsection (v) generally will apply because the retail value of the actual software is what the manufacturers would have reasonably received if a defendant's customers had lawfully purchased the software.

This approach focuses on the total harm caused to the victim and on the defendant's unjust enrichment, regardless of whether legitimate sales were displaced. *See id.* app. C (2000) (Amendments 590, 593); *United States v. Powell*, No. 05-4064, 2005 WL 1670608, at *1 (4th Cir. July 19, 2005) (affirming application of § 2B5.3(b) infringement amount where defendant argued that victim suffered "no pecuniary harm" or "loss" from copyright infringement).

The defense's "no lost sales" argument, on the other hand, ignores the value of the stolen software (and the related internal data stolen in the Crack99 case) to both the criminal and to its lawful owner. Dr. Best, for instance, was unjustly enriched by obtaining software that was worth over $2.3 million and was extremely valuable to him. He used it to design products as "Chief Scientist" for a government contractor.

The defense theory also ignores all components of value aside from sales price. For instance, the theory does not account for the victim-company's sunk costs in developing, licensing, and seeking to protect its product. Uncontrolled online dissemination of this software also might allow competitors to avoid the costs related to the research and development of similar software. It also may result in brand dilution over time. These are extremely serious concerns for software technology companies, particularly those with a limited offering of products that are the crown jewels of their businesses.

The defense theory also ignores the disincentive to invent tomorrow's products if they can be silently stolen and freely disseminated to all today. The value of today's businesses is inextricably tied to their digitized intellectual property. The Internet has made it very easy for those sitting across oceans to steal this intellectual property on a daily basis. Rampant digital looting of these crown jewels without consequence imperils the foundation of our modern economy and national security. There is thus much more at stake in the cyber-theft of intellectual property than the displacement of legitimate sales.

B. Responding to arguments based on culturally divergent views of cybercrime

Li's counsel argued that a cultural acceptance of cyber-theft of American technology in China should serve as a mitigating factor at sentencing. At first blush, this argument may sound ridiculous, particularly to this audience. Thematically, though, this argument mirrors the "dual criminality" concerns in extradition analyses. When one tacks on that it is the rare instance in which a foreign citizen is hailed into a U.S. court in shackles for something that is not criminally prosecuted in his country, the argument may seem somewhat more appealing.

It is an argument that must be forcefully rebutted. First, the facts of the case should be used to show that criminal intent is clear and the criminal conduct severe. The Government should prove that the defendant willfully flouted U.S. law to inflict significant harm on victims. Second, publicly available material (studies, congressional and other government sources, media reports, etc.) can be marshaled to show that cyber-theft of intellectual property from American companies poses an enormous economic and security threat to the United States. It therefore should compel a strong judicial response that seeks to promote international respect for U.S. law and to deter others from believing that cyber-looting of American companies is without consequence.

VI. Key victim issues

Working with victim-companies in international cybercrime cases is a time-consuming and complex process. It is also crucial to the success of these types of cases. Investigating and prosecuting cyber-based intellectual property crimes, in particular, requires significant victim involvement—from

providing access to devices or networks that are digital crime scenes, to analyzing and testifying about network intrusions and stolen intellectual property. For a variety of reasons, victim-companies may have widely divergent views on working with law enforcement agencies on cybercrime cases. Prosecutors and agents, therefore, must focus on developing strong, individual relationships with senior managers in victim-companies to maximize the potential for successful investigations and prosecutions. Even at the organizational level, a victim who trusts us is more likely to help us.

Understanding the organizational implications of cyber-theft is critical to developing strong, successful working relationships with victim-companies. These organizations are increasingly becoming targets of government regulatory investigations, civil litigation, and even congressional hearings geared toward creating greater cybersecurity and disclosure obligations. In many instances, a victim-company's enterprise value is heavily tied to creating and protecting its intellectual property. Many of them have boards of directors and investors to whom they must answer about negative cyber events. The current data security and privacy environment is also fraught with reputational risk for cybercrime victims. Moreover, there is the distinct possibility that the cybercrime at issue (or others like it) is ongoing, repeatable, and difficult to detect and remediate. Thus, unlike virtually any other type of crime victim, cyber-theft victims must immediately balance a host of competing concerns relating both to the crime itself and to the potential negative, external implications of the crime for their organizations.

Despite their traditional reluctance to notify law enforcement that they have been victimized by cybercriminals, more organizations are now doing so. This is likely due, in part, to the pervasiveness of these crimes and a more general acceptance that "everyone is getting hit" by cyber incidents. The regulatory landscape also continues to require greater disclosure of cyber events that impact certain types of data. For instance, export laws have long required any person "who knows or has reason to know of" any sale, export, transfer, re-export, or re-transfer of controlled technology to a prohibited nation (such as China, Iran, North Korea, Sudan, Syria, or Venezuela) to "immediately inform" the Department of State's Directorate of Defense Trade Controls. 22 C.F.R. § 126.1(a), (e) (2014). In November 2013, the Department of Defense instituted a rule requiring notification of any cyber event that affects "unclassified technical information" held on a contractor's (or its subcontractors') information systems. *See* Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011-D039), 78 Fed. Reg. 69273 (Nov. 18, 2013). Government contractors outside of the defense industry are facing similar issues. Numerous federal and state laws require disclosures relating to data breaches impacting different types of personally identifiable information. *See, e.g.*, Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 C.F.R. pt. 30 (OCC), pt. 208 (Federal Reserve System), pt. 364 (FDIC), pt. 568 (OTS) (financial account information); 45 C.F.R. § 164.314(a)(2)(1)(C), § 164.410 (personal health information); Rev. Proc. 97-22, 1997-1 C.D. 652, 1997-13 I.R.B. 9; Rev. Proc. 98-25 (taxpayer records); AM. BAR ASS'N, THE ABA CYBERSECURITY HANDBOOK App'x B.5 (listing state data breach notification laws). These trends will likely continue to accelerate along with the breadth and depth of the cybercrimes that drive them.

Regardless of legal notification requirements, our best approach continues to be building strong, individual relationships with senior managers within victim organizations—before a cyber-incident occurs, where possible. As the Crack99 case illustrates, a victim that has an individual relationship with particular agents or prosecutors may provide information that serves as the impetus for launching an investigation. This seems particularly true in the intellectual property theft context, where a victim-company may not be legally required to disclose cyber-thefts. A personal relationship also may lead to much greater cooperation as an investigation progresses.

In the Crack99 case, we worked extensively with about 20 victim-companies (roughly 10 percent of the total victims) that had software stolen, cracked, and distributed online. Following the victim-company disclosure that launched the investigation, we began working with a number of these victims as we conducted undercover purchases of their software. Many of them provided us with technical analyses

of their products and data that we recovered. Some also provided analyses or information concerning the impact of this and similar crimes on their businesses. Other companies became involved at the sentencing phase after publicity surrounding the convictions spread. We collected and used sensitive and proprietary business data (but only that which was absolutely necessary) pursuant to protective orders similar to those used in civil intellectual property litigation. We provided the companies with as much information as we could, as soon as we could, about the overall crime and the involvement of their products in it. After sentencing, we also provided them with lists of the Crack99 customers who had unlawfully obtained their products.

In addition to the importance of building a strong, individual relationship with senior managers within organizations, some other considerations in working with organizational victims of cybercrime are provided below.

- Coordination with victim-companies should not be left entirely to agents. Instead, prosecutors should engage senior management within victim-companies early in cases, consistent with investigative sensitivities. Responding to cyber-events is often a multi-disciplinary task inside of an organization. Internal and external lawyers, business managers, IT specialists, and communications personnel are likely to be involved. Finding good senior contacts may ensure that key information is being shared appropriately. It also may ensure that decisions made by the organization as to the investigation are properly authorized. Finally, sharing information with senior managers may aid in maintaining a cooperative relationship throughout the case.
- A careful approach must be taken in terms of the timing and amount of information sharing that occurs. In multi-victim cases, that approach may vary by victim. The needs of the criminal investigation and considerations relating to mitigating ongoing cyber threats should be given primacy. Remediating losses and preventing future crimes should be considered as well. During a case, victims should be kept informed of the progress of an investigation. Advance notice and consultation about significant events (charges, pleas, sentencing recommendations, etc.) aids in building strong, productive relationships with organizational victims.
- Advance coordination of the public release of case information is highly desirable. Coordinating our public statements with the victim-company may prevent the needless disclosure of information that may be harmful to the company. Where reputational or other harm may result, we can provide the company with an opportunity to prepare for and best manage that issue. In return, we can ask victims to provide us with advance notice of public statements that they may issue. Such statements may become very important at any trial or sentencing phase.
- Investigations into a victim-company's networks or devices should be done in a way that minimizes business disruption and exposure of data beyond that relevant to the investigation.
- It is in our best interest to allow victim-companies to share their expertise about the technical aspects of the crime and the impact of it on their businesses. We ultimately will be able to tell the story much better with their input and guidance.
- Protecting information and data provided by the victim-company from disclosure to defendants, other criminals, or the company's competitors or customers, must be a top priority.
- Consistent with case sensitivities, we should attempt to provide victim-companies with information that they can use to make any required disclosures to other government components or private parties.
- Maintaining relationships with company representatives after a case concludes may lead to the next great cyber case.

VII. Conclusion

International cybercrime cases are time-consuming, complex investigations with no guarantee of success. They are often more dynamic than, and involve equities that do not exist in, most domestic criminal cases. They are also critically necessary responses to the explosive growth of foreign-based cyber-theft of intellectual property and personally identifiable information from American organizations. We can and we should prosecute more international cybercriminals.

In pursuing cybercriminals across the globe, consider these concluding thoughts taken from the Crack99 and other cyber-theft cases:

- Private sector outreach is critical to fostering the relationships that create many of the best opportunities to develop successful international cybercrime cases.
- New and old investigative techniques can be combined to identify and apprehend members of international cybercrime groups, otherwise known only by their Internet connections and devices.
- Be prepared to invest years in successfully investigating and prosecuting these targets.
- It is absolutely possible to apprehend criminals who commit all of their cybercrimes in countries that have no extradition treaties with the United States.
- Prosecutors must think carefully through extradition implications when selecting charges and before any extradition process begins.
- In addition to more traditional crimes, cyber intrusions and intellectual property theft also may be export control crimes.
- Video-recorded undercover meetings provide the type of evidence that can seal a cybercriminal's fate at trial and sentencing.
- Dismantling digital architecture is necessary to fully disrupting criminal activity even after a target is in custody.
- Investigating organizational managers and their operations will likely lead to identifying many viable targets for prosecution. These targets may prove to be much more than low-level offenders.
- Sentencing issues can be complicated by "actual loss" arguments and a dearth of strong sentencing precedent for international cybercrime cases, particularly in the intellectual property context.
- Dealing with victim-companies is a complex and critically important process that requires significant time and understanding of the organizational implications of cybercrime. ❖

ABOUT THE AUTHOR

❑ **Edward J. McAndrew** is an Assistant U.S. Attorney in the District of Delaware, where he focuses on Internet-based and technology facilitated crimes. He previously served in the Cyber Crime Unit of the Eastern District of Virginia and in the Criminal Division's Child Exploitation and Obscenity Section. Prior to joining the Department in 2006, he was a litigation partner and the Deputy Practice Group Leader of Reed Smith LLP's Global Regulatory Enforcement Group. ✠

The Degree of Fourth Amendment Protections Afforded to Foreign Searches

Mi Yung Park
Trial Attorney
Child Exploitation and Obscenity Section
Criminal Division

Globalization and information technology advances have resulted in an increase in prosecutions that rely on evidence obtained outside of the United States. As a result, prosecutors and courts are grappling with more frequent and complex questions about the constitutional protections that apply to evidence gathered overseas. This article discusses in detail the applicability of the Fourth Amendment to foreign searches, including the foreign use of electronic technology in securing evidence, as well as to the electronic media seized.

I. Fourth Amendment applicability: "substantial participation" required

As a general rule, evidence obtained by foreign police officers from searches carried out in their own countries is admissible in U.S. courts, regardless of compliance with the Fourth Amendment. *United States v. Barona*, 56 F.3d 1087, 1090–91 (9th Cir. 1995) (analyzing the validity of a foreign wiretap); *United States v. Behety*, 32 F.3d 503, 510 (11th Cir. 1994); *United States v. Heller*, 625 F.2d 594, 599 (5th Cir. 1980). Constitutional protections, however, will be provided where U.S. law enforcement officials substantially participated in a search in the foreign nation, or the foreign officials conducting the search were acting as agents of the U.S. Government. Some courts, and in particular the Ninth Circuit, have dubbed this as the "joint venture" doctrine. *Stonehill v. United States*, 405 F.2d 738, 743 (9th Cir. 1968) ("If Federal agents [have] so substantially participated in the raids so as to convert them into joint ventures between the United States and the foreign officials," then the exclusionary rule may apply.).

Courts usually apply a relatively high threshold for a finding of "substantial participation" to warrant Fourth Amendment protection. U.S. law enforcement's mere participation in some capacity in a foreign-led search, such as by providing the initial information or being present for the search, will likely not be found to be so extensive as to warrant Fourth Amendment protection. *See Behety*, 32 F.3d at 506–07; *United States v. Maturo*, 982 F.2d 57, 59–62 (2d Cir. 1992) (no finding of U.S. substantial participation even where foreign officials utilized wiretaps and provided copies of the recordings to U.S. agents); *United States v. Hawkins*, 661 F.2d 436, 456 (5th Cir. 1981); *United States v. Marzano*, 537 F.2d 257, 270 (7th Cir. 1976) (abrogated on other grounds); *Stonehill v. United States*, 405 F.2d 738, 746 (9th Cir. 1968); *but see United States v. Peterson*, 812 F.2d 486, 490 (9th Cir. 1987) (joint venture existed in drug trafficking case where U.S. agents were involved in daily translating and decoding of intercepted transmissions, advised the foreign authorities about the relevance of the transmissions, and treated the drugs as destined for the United States).

Courts have applied these legal standards in a number of recent federal child exploitation prosecutions in which foreign evidence has been used. In most cases, these courts have found that there was no "substantial participation" by the U.S. Government. *See United States v. Frank*, 599 F.3d 1221, 1228–29 (11th Cir. 2010) ("At all times, the Cambodian officers acted out of their own interest" and there

was "no evidence that the Cambodian officers acted as agents of the United States."); *United States v. Flath*, 845 F. Supp. 2d 951, 957–59 (E.D. Wis. 2012) (no substantial participation where U.S. officers provided initial information and, although present for the foreign search of the U.S. citizen's residence, did not actively participate in the search of the foreign residence or the ultimate seizure of computers and electronic media from that residence). In some cases, however, courts have determined that U.S. law enforcement participation in an investigation was sufficient to trigger some Fourth Amendment protections. *See, e.g.*, *United States v. Stokes*, 710 F. Supp. 2d 689, 697 (N.D. Ill. 2009) (in addressing the defendant's motion to suppress electronic evidence seized from his foreign residence, the court found the existence of substantial participation to implicate Fourth Amendment protections where U.S. law enforcement was actively involved in both the foreign search and investigation leading up to the search).

It is important to be aware that where foreign conduct involves both a suspect's interview and a search of premises, thus implicating both Fourth and Fifth Amendment concerns, separate analyses of substantial participation by U.S. law enforcement should be conducted. That is, a court may find that U.S. law enforcement substantially participated in a suspect's foreign interview, thus implicating the Fifth Amendment, but did not participate substantially in the foreign search of the residence of that same suspect so as to implicate the Fourth Amendment. *See Flath*, 845 F. Supp. 2d at 959 ("[T]he fact that the U.S. officer's interrogation could be categorized as substantial has no bearing on this court's inquiry into whether the U.S. officers' participation in the search was substantial."). Not every court will necessarily conduct such separate analyses, so it is advisable that the court is made aware of this difference. *Compare United States v. Mundt*, 508 F.2d 904, 906–07 (10th Cir. 1974) (where U.S. officers substantially participated only in events leading up to the arrest, *Miranda* not implicated), *with United States v. Emery*, 591 F.2d 1266, 1268 (9th Cir. 1978) (court considered substantial participation of U.S. agents leading up to the arrest in finding that a joint venture existed and that Fifth Amendment applied to subsequent interview).

II. If "substantial participation" is found

It is next important to discuss in what way the Fourth Amendment applies to a foreign search when constitutional protections are triggered by the substantial participation of U.S. authorities.

A. The Fourth Amendment

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

The Fourth Amendment contains two separate clauses that are independent of each other. *See United States v. Barona*, 56 F.3d 1087, 1092 n.1 (9th Cir. 1995). The first part of the Fourth Amendment prohibits "unreasonable" searches and seizures, while the second clause, more commonly known as the "Warrant Clause," describes the procedures to be followed in obtaining a search warrant. *Id.*

B. Warrant Clause inapplicable

Given the sovereignty of each nation to create its own laws and procedures of implementation, it would be unworkable to apply the Warrant Clause or its probable cause standard to foreign searches. The Second Circuit has explicitly held that the Warrant Clause of the Fourth Amendment does not apply extraterritorially. *See In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 167 (2d Cir. 2008) (involving evidence obtained through electronic surveillance conducted by foreign officials). The Ninth Circuit implicitly reached the same conclusion when it noted that "foreign searches have neither

been historically subject to the warrant procedure, nor could they be as a practical matter." *Barona*, 56 F.3d at 1092 n.1. Moreover, while the Supreme Court has not ruled on this issue, it has strongly suggested that the Warrant Clause does not apply to overseas searches because a warrant "would be a dead letter outside the United States." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274 (1990).

Even if the Warrant Clause does not apply extraterritorially, would the Fourth Amendment require a foreign search to be supported by probable cause? The relevant cases suggest not. For example, the majority in *Barona* noted that the Supreme Court in *Verdugo* "expressly rejected the very conclusion—that a foreign search must be based on probable cause even if no warrant is required." *Barona*, 56 F.3d at 1092 n.1. Rather, "[r]easonableness, not probable cause, is undoubtedly the touchstone of the Fourth Amendment" such that "although 'both the concept of probable cause and the requirement of a warrant bear on the reasonableness of a search . . . in certain limited circumstances neither is required.' " *Id.* (citing *New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985)); *see also In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d at 168 ("[B]ecause the ultimate touchstone of the Fourth Amendment is reasonableness, the warrant requirement is subject to certain exceptions.") (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)) (internal quotations omitted).

C. Reasonableness: Compliance with foreign law or totality of the circumstances?

Where a court finds substantial participation by the U.S. Government and Fourth Amendment protections are thus implicated in a foreign search, only the Fourth Amendment's reasonableness requirement must be met. *In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d at 171; *United States v. Juda*, 46 F.3d 961, 968 (9th Cir. 1995); *see also Flath*, 845 F. Supp. 2d at 960; *Stokes*, 710 F. Supp. 2d at 700 (determining whether a warrant was reasonable under the Fourth Amendment where both the U.S. and foreign governments participated in the search).

What constitutes a reasonable foreign search under the Fourth Amendment varies by circuit, and most circuits have not addressed this narrow issue. Only the Ninth and Second Circuit have clearly set forth when a foreign search fulfills the Fourth Amendment's reasonableness standard.

The Ninth Circuit held that where U.S. law enforcement substantially participated in a foreign search to implicate the Fourth Amendment, the reasonableness of the search is determined by assessing compliance with foreign law. *Juda*, 46 F.3d at 968 ("[A] foreign search is reasonable if it conforms to the requirements of foreign law."). Thus, "compliance with foreign law alone determines whether the search violated the Fourth Amendment." *Barona*, 56 F.3d at 1093 n.1, 1095 (admitting foreign evidence because the court was "satisfied that Danish law was followed"); *United States v. Pepe* (Pepe Minute Order), CR 07-168-DSF (C.D. Cal. filed Feb. 7, 2008) (compliance with Cambodian law sufficient to satisfy the requirements of the Fourth Amendment in determining reasonableness of foreign search of foreign residence and the contents of computers and computer media contained within that residence).

The Second Circuit reviews the totality of the circumstances surrounding the foreign search to determine whether the search was conducted reasonably. *In re Terrorist Bombings of the U.S. Embassies in E. Africa*, 552 F.3d at 172. District courts within the Seventh Circuit have followed the Second Circuit and applied the totality of the circumstances test to measure whether the foreign search was conducted reasonably. *See Flath*, 845 F. Supp. 2d at 960–61 ("Reasonableness [under the Fourth Amendment] is measured in objective terms by examining the totality of the circumstances."); *Stokes*, 710 F. Supp. 2d at 701 ("To determine whether a [foreign] search is reasonable under the Fourth Amendment, the court must examine the totality of the circumstances, balancing 'on the one hand, the degree to which it intrudes upon the individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.' ") (citing *Samson v. California*, 547 U.S. 842, 848 (2006)).

While not the sole factor, these courts assessing the totality of the circumstances have also considered the degree of compliance with foreign law as one factor among many to determine whether a foreign search complied with the reasonableness requirement of the Fourth Amendment. *See In re*

Terrorist Bombings of the U.S. Embassies in E. Africa, 552 F.3d at 173–74 (one factor considered in the totality of the circumstances test was that the foreign search was not conducted covertly, but rather pursuant to a valid foreign search warrant); *Flath*, 845 F. Supp. 2d at 960–61; *Stokes*, 710 F. Supp. 2d at 701.

Generally, "[t]he proponent of a motion to suppress has the burden of establishing that his own Fourth Amendment rights were violated by the challenged search or seizure." *Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978). There is nothing to suggest that this general rule would not extend to challenges to foreign searches, and the defense bears the burden of proving a violation of the applicable foreign law. *See United States v. Morrow*, 537 F.2d 120, 140 (5th Cir. 1976) (rejecting the idea that in a foreign search context, the Government bears the burden of proving compliance with foreign law); Pepe Minute Order, at 5 (finding that the defendant had not carried his burden of demonstrating that the search violated Cambodian law).

D. Good faith exception

Even when a court determines that a foreign search violates the Fourth Amendment's reasonableness standard, foreign evidence has still been admitted under the good faith exception to the exclusionary rule when a court has found that the involved U.S. officers reasonably relied on representations made by foreign officers. *See Juda*, 46 F.3d at 968; *Peterson*, 812 F.2d at 492; *Stokes*, 710 F. Supp. 2d at 702; *United States v. Ferguson*, 508 F. Supp. 2d 1, 6 (D.D.C. 2007) (finding that even if the Fourth Amendment had applied to the foreign wiretaps, "[t]he good faith exception . . . applies if United States law enforcement agents have a reasonable belief that the foreign nation's laws were complied with").

As noted by one court, "[t]his extension of the good-faith exception accommodates the special circumstances presented to U.S. law enforcement officials when conducting a search in a foreign country: the lack of familiarity with foreign procedures and foreign law, and the difficulty of imposing the law of the United States on foreign officials." *United States v. Staino*, 690 F. Supp. 406, 410–11 (E.D. Pa. 1988) (citing *Peterson*, 812 F.2d at 492); *see also United States v. Vilar*, No. S305CR621KMK, 2007 WL 1075041, at *58 (S.D.N.Y. Apr. 4, 2007) (noting that "[i]n a typical extraterritorial search . . . 'American law enforcement officers [are] not in an advantageous position to judge whether the search was lawful,' and '[h]olding them to a strict liability standard for failings of their foreign associates would be even more incongruous than holding [them] to a strict liability standard as to the adequacy of domestic warrants' ") (quoting *Peterson*, 812 F.2d at 492).

The *Pepe* court, citing to *Peterson*, extended the good faith exception to implicit representations by foreign officers and found that, "[i]t was not 'objectively unreasonable' for [the U.S. officer] to rely on the implicit assertion that such a search would comply with Cambodian law." Pepe Minute Order, at 6 (discussing search of defendant's computer by U.S. officials pursuant to a request by Cambodian officials); *accord Vilar*, 2007 WL 1075041, at *58 ("[T]here is no basis in the law to have required [the U.S. official] . . . to make a potentially undiplomatic inquiry into the propriety of [the foreign official's] decision . . . or to demand that she see the application papers."). However, if possible, obtaining an explicit representation regarding compliance of foreign law is the suggested practice.

Additionally, the Government should point out that where the exclusionary rule "does not result in appreciable deterrence . . . its use . . . is unwarranted." *United States v. Leon*, 468 U.S. 897, 909 (1984) (citing *United States v. Janis*, 428 U.S. 433, 454 (1976)). The D.C. Circuit explained:

> The exclusion of evidence by American courts because the evidence was deemed obtained in objectionable ways would in no way deter conduct by foreign police acting in their own countries for their own reasons. In such cases, exclusion under the supervisory power would be improper since it would seriously alter the balance the Court has already

> struck between the "need to deter . . . underlying [mis]conduct and the detrimental impact of excluding . . . evidence."

United States v. Mount, 757 F.2d 1315, 1321 (D.C. Cir. 1985) (quoting *United States v. Payner*, 447 U.S. 727, 736 (1980)); *United States v. Andreas*, No. 96 CR 762, 1998 WL 42261, at *2 (N.D. Ill. Jan. 30, 1998) (The court in determining the admissibility of evidence seized by foreign officials "must inquire whether exclusion will deter federal officers from unlawful conduct.") (citing *Peterson*, 812 F.2d at 491); *United States v. Molina-Chacon*, 627 F. Supp. 1253, 1259 (E.D.N.Y. 1986) (In analyzing a foreign search, the court should be mindful that "[t]he guiding principle is that the exclusionary rule is not a constitutional right of an individual but rather a judicially created device to deter United States police misconduct, to be applied only in those situations where this objective can be achieved.") (citing *Janis*, 428 U.S. at 446–47).

As the Supreme Court has emphasized, "exclusion has always been our last resort, not our first impulse . . . and applies only where it results in appreciable deterrence." *Herring v. United States*, 555 U.S. 135, 140 (2009) (internal quotations omitted). Moreover, the Supreme Court has clarified that it has "never suggested that the exclusionary rule must apply in every circumstance in which it might provide marginal deterrence" but that "to the extent that application of the exclusionary rule could provide some incremental deterrent, that possible benefit must be weighed against [its] substantial social costs." *Id.* at 141 (internal quotations omitted).

Suppression of foreign evidence for a Fourth Amendment violation is an extreme measure and, as the Second Circuit has noted,

> [t]here exists no case, so far as we are aware, which suppresses evidence obtained in a foreign country under such conditions, regardless of whether the foreign officers failed to follow American constitutional procedures or of the extent to which American agents may have been involved in their activities. The courts can hardly be said to have spoken with one voice in articulating the reasons for their decisions, but as a statistical matter they have apparently been unanimous in rejecting attempts to suppress the challenged foreign evidence.

United States v. Molina-Chacon, 627 F. Supp. 1253, 1259 (E.D.N.Y. 1986) (citing *Stowe v. Devoy*, 588 F.2d 336, 342 (2d Cir. 1978)).

III. Conclusion

While only a handful of courts have addressed the scope of Fourth Amendment protection afforded to foreign searches, they have all consistently found that only the reasonableness requirement of the Fourth Amendment applies. Addressing early in the investigation the issues specific to the evidence and the foreign country involved can reduce the chances that a defense motion to suppress will succeed and the evidence gathered be suppressed. Prosecutors should consider consulting with the foreign country either informally, through the U.S. agents assigned to that country, or more formally, through the Department of Justice Office of International Affairs, to determine the foreign country's willingness and ability to provide assistance regarding the facts of the foreign search/interview and the governing foreign law.❖

ABOUT THE AUTHOR

❑ **Mi Yung Park** is a Trial Attorney with the Child Exploitation and Obscenity Section (CEOS) in the Criminal Division at the Department of Justice, where she prosecutes federal child exploitation statutes. Prior to joining CEOS, Ms. Park worked as an Assistant U.S. Attorney for the U.S. Attorney's Office in San Diego and focused on the prosecution of narcotics and criminal immigration cases. She also worked at the Civil Rights Division at the Department of Justice, where she enforced civil federal voting laws. ✠

Eenie, Meenie, Miney, Mo: Choosing and Working With an Expert in a Stolen Trade Secrets Case

Scott L. Garland
Assistant United States Attorney
District of Massachusetts

I. Introduction

One of the most enjoyable aspects of investigating the theft of a trade secret—whether under the trade secret statutes, 18 U.S.C. §§ 1831 and 1832, or the mail and wire fraud statutes, 18 U.S.C. §§ 1341 and 1343—is learning about the technology. Technology fascinates me if only because, like so many other lawyers, I was never successful at building anything useful myself. Investigations into the theft of trade secrets can teach you about technologies that otherwise would remain a mystery. My own trade secret investigations have taught me about designing and producing microprocessors, X-rays, sintering powdered metal into solid auto parts, and the considerations factoring into the business decision to have someone else host your Web site. And that does not even scratch the surface of the technologies implicated in trade secret litigation. *See* DEP'T OF JUSTICE, PROSECUTING INTELLECTUAL PROPERTY CRIMES 164 (4th ed. 2013) (collecting cases involving trade secrets relating to anti-cancer drug, aircraft brake assembly, adhesives, computer source code, Coca-Cola products, a tire-assembly machine, and others).

This article considers how to work with experts to determine whether in your investigation a trade secret exists, how to find the best and most appropriate expert for your case, and addresses subjects and problems that will arise in your expert's preparation and testimony.

II. Defining and identifying a trade secret

The definition of "trade secret" is very broad. *See id.* at 162–63 (citing *ConFold Pac., Inc. v. Polaris Indus*, 433 F.3d 952, 957 (7th Cir. 2006) (noting that a trade secret can be any information, whether in tangible form or otherwise, that its owner takes reasonable measures to keep secret and that has some economic value as a result of its secrecy). For purposes of federal criminal prosecution, a trade secret is any type

> 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, and not being readily ascertainable through proper means by, the public.

18 U.S.C. § 1839(3) (2014). In plain English, a trade secret is information that is used for business purposes, that its owner used reasonable means to keep secret, and that is valuable because other people do not know it and cannot easily figure it out. In even plainer English,

> A trade secret is really just a piece of information (such as a customer list, or a method of production, or a secret formula for a soft drink) that the holder tries to keep secret by executing confidentiality agreements with employees and others and by hiding the information from outsiders by means of fences, safes, encryption, and other means of concealment, so that the only way the secret can be unmasked is by a breach of contract or a tort.

ConFold Pac., 433 F.3d at 959. (Although this definition comes from a civil case interpreting state trade secret law, it applies equally to federal criminal law.)

Common defenses are that the owner did too little to keep the information secret, that the information had already been disclosed publicly, and that a competitor figured out the information on its own without taking any improper steps, or could have done so without much difficulty. *See* DEP'T OF JUSTICE, PROSECUTING INTELLECTUAL PROPERTY CRIMES 193–201 (4th ed. 2013).

Although one of the most enjoyable aspects of a trade secret investigation is learning about the technology, one of the most difficult aspects is determining which part of the technology is a trade secret, how to prove that it fits the legal definition, and how to disprove the common defenses. Start with determining what precisely the trade secret is. Typically, the corporate victim brings you a collection of computer files that the suspect downloaded and says, "Of course these are trade secrets: see how much he took and how complicated it looks?" Narrowing this information down to exactly which part of a stolen document or product sample is a trade secret may require a great deal of thought and consideration. Is it the whole document or a particular section, page, graph, drawing, paragraph, sentence, equation, or number within an equation? Is it the product itself or how the product is manufactured? Asking these questions in these terms sometimes prompts a helpful answer. More often, I get a better answer by asking the witness to "show me where the magic happens." They get it.

Once you have narrowed it down to where the magic happens, you should ask, How do I prove that it truly is a secret and has some value because of its secrecy? In other words, How do I prove the negative proposition that the "secret" was never disclosed and could not have been figured out through lawful means by someone without access to the "secret"? *See* 18 U.S.C. § 1839(3)(B) (2014). To answer the secrecy question, ask witnesses whether they have discussed the "secret" at trade conferences, published it in papers, included it in public patent applications, posted it on their Web site, discussed it in their advertising or marketing materials, seen it discussed in trade publications, seen it used by competitors or former employers, or merely seen it discussed on the Internet. To answer the question about how easy it would be for someone else to figure out the "secret" on their own, ask them how long and how much money it would take their competitor to figure out the "secret" if they really set their mind to it.

The next item to consider is how far as a prosecutor you want to go in fighting defense counsel about whether a particular piece of information qualifies as a trade secret. Christopher Merriam, an

Assistant Deputy Chief at the Department of Justice's Computer Crime and Intellectual Property Section, used to tell me that if the main issue in a criminal trade secret case is whether the trade secret qualifies as a trade secret, the Government has already likely lost its case. A fight about the trade secret detracts from what should be the main issue: the defendant's intent in taking it.

But that does not mean that you can skip learning what the trade secret is and why it qualifies, or that you should not fight to prove the trade secret's validity against the defendant's natural defense of "nuh uh."

III. Finding your expert

Determining whether a technology is a trade secret requires bringing in someone whom you trust on this point. This person will naturally be some type of expert. The best expert has excellent technical credentials and is someone who, more importantly, can recharacterize complicated technology into simple metaphors and analogies. Through these metaphors and analogies, they reduce the technology into something understandable for the average juror (and lawyer), and allow the case to focus on the defendant's intent.

But where do you find that expert? Industry? Academia? The victim? Somewhere else? The answer may not be obvious.

A. Outside expert

There are many problems to consider with getting guidance from an outside expert. When we look for an expert, we want someone who has broad experience. But many trade secrets are not discussed broadly because, by definition, they must be kept secret within a company. The number of people who have firsthand experience with multiple companies' trade secrets may be fairly limited. This situation is especially true of newer technologies and industries, which may have few companies, academics, or established standards. Of course, because of the opportunity to get in on the ground floor, newer technology and industries may offer the best trade secrets to steal.

The cost of an outside expert is also a consideration. As the budgets of U.S. Attorneys' offices contract, prosecutors may lack sufficient money to pay for experts. A well-qualified expert can come at a high hourly price. Combing through the hundreds, if not thousands, of documents that modern computer technology allows people to steal can be time-consuming and thus, costly.

Another issue is allaying the victim company's fear that an outside expert will look at the stolen technology, turn around, and use it to compete against their company. The victim reported the theft in the first place because it wanted its trade secrets kept secret. It will naturally worry that the litigation itself will expose the trade secret to the world. The way to allay this fear is with a confidentiality/nondisclosure agreement, discussed in section IV of this article. But in high-technology cases, you may need a special restriction, a "patent prosecution bar," the terms of which could complicate hiring an outside expert.

B. Victim's employees

If not an outside expert, then who? The victim's own employees are a good place to start. After all, when you first open an investigation, the people who show you the trade secret will likely be the victim company's employees. They have the most familiarity with the company's documents, processes, and know-how. They have the biggest stake in the investigation. They should be your default experts.

This is not, however, as easy as it sounds. Which employees should you rely on? You might have a choice of the people who actually use the purported trade secret versus the people who developed it. They might come from different parts of the organizational pyramid, either higher or lower in the hierarchy, or from different divisions. They might have different views about what is valuable due to their

different education, familiarity, and experience with the technology. They might also have different views and experiences concerning whether the information is or should be kept secret. They might go to different conferences and trade shows and have different conversations about the technology with colleagues in competing companies. The view from the ivory tower may differ significantly from the view on the shop floor. Your job is to determine which view is the most accurate.

Another issue with using your victim company's employee as an expert is that if the employee-expert is less articulate or likeable than you prefer, he or she might be difficult to "fire" from the litigation team. Discussing this problem with the victim company can be awkward. The company might insist that you use the flawed employee in any event. You need not comply, but the awkwardness can still persist.

A final issue with using the victim employee as an expert is, of course, the issue of bias. Bias is a real concern. The employee owes his allegiance—his livelihood, in fact—to the victim company. How could he be expected to testify against his employer's interest? But think of the alternative: the outside expert who has been hired specifically for this litigation. Which expert is the jury more likely to find biased: the victim's employee or the outside expert? It might be a toss-up. Whereas the outside expert's academic or employment credentials might be more neutral, the victim's employee might testify in a manner that personalizes the victim company, which could otherwise appear to be an impersonal corporate Goliath against the defendant's David.

Of course, this is not an either/or proposition. You might want expert testimony from not only the victim's employees, but also an outside expert.

C. The magical expert

What if you could use an expert who has all the benefits of both the outside expert and the victim's employee, but without any of their drawbacks? What if the expert has all the requisite know-how, but without considerable expense and bias? What if, in fact, he or she could testify with the opposite of bias? That is, what if the expert could testify for the Government despite having business interests opposed to the victim company? Wouldn't that be an expert you would like to present?

Who is this magical expert? The victim company's business competitor.

Imagine that Best Widget Company accuses the defendant of taking its trade secrets and that Best Widget's biggest competitor is Widgets America. Chances are that both companies use similar (but not identical) types of technology and that both companies want their respective technological details kept secret. Because of these aligning organizational interests, chances are that Widgets America will agree with Best Widget Company that the stolen documents include trade secrets. If Widgets America disagrees, then your problem might not be in locating an expert, but rather in having picked the wrong trade secret.

How do you show trade secrets owned by Best Widget to Widgets America without putting Best Widget out of business? One answer is redacted documents. You ask Best Widget to identify their trade secrets and redact them to the finest point of granularity possible. For example, Best Widget should not redact the entire equation if redacting the equation's constant will do. With documents suitably redacted, you can show them to business competitors, to defense experts, to juries, even to reporters without a concern. These redacted documents could even become your trial exhibits. In fact, in a suitable case, if certain discovery is restricted to redacted documents, you might obviate the need for a patent prosecution bar. *See* section IV of this article.

This tactic will not always work. Sometimes the redaction itself would give away the game. For example, if the trade secret involves making a peanut butter sandwich, redacting the peanut butter's salt content might suffice, whereas redacting the addition of cinnamon might not. Sometimes the redaction results in talking about too much white-space.

In a recent important investigation, however, it worked. The defendant stole trade secrets from his employer, Company A, and then took a job with the employer's biggest competitor, Company B. We quickly determined that the defendant had done so without Company B's knowledge, and noted that in the indictment. We worked with Company A, the victim, to narrow down the boxes and boxes of documents that the defendant took and created about 40 short potential trade secret exhibits. Each potential exhibit included the document's title page, table of contents, and excerpts that included trade secrets, the particulars of which were redacted. We then showed these redacted exhibits to Company B, the competitor, with Company A's approval. When Company A and Company B disagreed about whether a potential exhibit contained a trade secret, we planned not to use it at trial. When the companies agreed, however, that a potential exhibit contained a trade secret, we planned to use it at trial because the defendant and his experts would have little credibility if they disagreed. Both companies' employees were on the witness list to testify about these trade secret exhibits at trial. We never hired an outside expert. The defendant eventually pleaded guilty.

IV. Avoiding the trade secret's misuse and disclosure by the expert

Giving a trade secret to an outside expert—whether hired by the Government or the defense—threatens that secrecy. How can you protect against this threat?

The standard answer is a confidentiality/nondisclosure agreement with the Government's expert and a protective order against the defendant's expert. In normal criminal litigation, a protective order is governed by Federal Rule of Criminal Procedure 16(d). In criminal trade secret litigation, a protective order is also governed by 18 U.S.C. § 1835, which states,

> In any prosecution or other proceeding under this chapter, the 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 requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

18 U.S.C. § 1835 (2014).

The standard confidentiality agreement or protective order prohibits the expert from using the disclosed documents for any purpose other than preparing for litigation. Other standard conditions prohibit the expert from giving the documents to others without prior approval and from storing them in a manner vulnerable to theft via a physical or Internet security breach. In other words, what happens in litigation-world stays in litigation-world.

But the standard terms of "for litigation purposes only" may not be enough. Relying on the expert to mentally quarantine any litigation-derived information from his or her other professional activities could be futile:

> Typically, protective orders include provisions specifying that designated confidential information may be used only for purposes of the current litigation. Such provisions are generally accepted as an effective way of protecting sensitive information while granting trial counsel limited access to it for purposes of the litigation. *Courts have recognized, however, that there may be circumstances in which even the most rigorous efforts of the recipient of such information to preserve confidentiality in compliance with the provisions of such a protective order may not prevent inadvertent compromise. . . . It is very difficult for the human mind to compartmentalize and selectively suppress information once learned, no matter how well-intentioned the effort may be to do so.*

In re Deutsche Bank Trust Co. Americas, 605 F.3d 1373, 1378 (Fed. Cir. 2010) (emphasis added) (internal quotation marks and alterations omitted) (citing *Fed. Trade Comm'n v. Exxon Corp.*, 636 F.2d 1336, 1350 (D.C. Cir. 1980)) (reviewing discovery order in patent litigation).

This poses a problem with an expert who is active in the world of patents. What do civil patent rights have to do with criminal trade secret litigation? Potentially everything. Your victim worries about losing the use or value of its trade secret to an expert who intentionally or inadvertently blocks the way with a competing patent.

> A patent is an intellectual property right granted by the Government of the United States of America to an inventor *to exclude others from making, using, offering for sale, or selling the invention* throughout the United States or importing the invention into the United States for a limited time in exchange for public disclosure of the invention when the patent is granted.

See USPTO.GOV, http://www.uspto.gov/patents/ (emphasis added) (internal quotation marks omitted). The competing patent could be as bad as the original theft, if not worse.

In addition to the standard provision in a confidentiality agreement or standard protective order that prohibits the expert from using the trade secret for anything other than litigation, the victim might insist that the expert not prosecute any patents relevant to the technology. This prohibition is common in high-technology litigation and is called a "patent prosecution bar." (In this context, "patent prosecution" does not mean penalizing someone for a criminal violation of patent rights, but rather obtaining a patent from the United States Patent and Trademark Office.). Whereas a standard protective order says "thou shalt not use the trade secret," a patent prosecution bar says "thou shalt not even apply for a patent in that area during the litigation, whether you think you are using the trade secret or not." In fact, patent prosecution bars can apply both to experts and lawyers. *See Eon Corp. IP Holdings, LLC v. AT&T Mobility LLC*, 881 F. Supp. 2d 254, 258–59 (D.P.R. 2012) ("Plaintiff argues that the bar, if imposed, should apply only to counsel, but we see no reason why the concerns motivating the prosecution bar—risk of inadvertent disclosure—would not also apply to experts or technical advisers."); *see also Applied Signal Tech., Inc. v. Emerging Markets Communications, Inc.*, No. C-09-02180, 2011 WL 197811, at *5 (N.D. Cal. Jan. 20, 2011) ("Allowing experts who prosecute patents themselves to access confidential technical information *without* the protection of a prosecution bar thus poses a tremendous risk of inadvertent disclosure."). The bar usually lasts through the litigation, plus a year or so thereafter. These outside experts might resist, because submitting to the bar could affect their research and income.

In *United States v. Pani*, the defendant was accused of stealing trade secrets concerning computer microprocessors that the victim had valued at hundreds of millions of dollars. *United States v. Pani*, No. 08-40034-FDS, 2010 WL 3928681, at *1 (D. Mass. Oct. 4, 2010) (denying criminal defendant's motion to weaken patent prosecution bar to cover only patent-related use of the victim's discovery information, rather than a categorical bar against prosecution common in civil cases). Pani eventually pleaded guilty to wire fraud and was sentenced to restitution and three years of imprisonment. His appeal of the technology's valuation for purposes of restitution and the Sentencing Guidelines is still pending.

Early in the case, the Government, represented by Assistant U.S. Attorney Adam Bookbinder and myself, moved for a patent prosecution bar against the defendant's experts. The defendant resisted, noting the difficulty he might have in locating a suitable expert. The court explained why the patent prosecution bar was necessary to protect the victim:

> The information submitted by the Government and Intel persuades the Court that at least some of the information allegedly stolen by the Defendant—the information that the protective order guards—is current (i.e. not outdated) highly technical information set out, at least in some documents, in great detail. Intel had also taken substantial steps to protect the information, which would appear to have a significant competitive value. A

> patent bar as compared to a prohibition on direct/indirect use provides a clearer line both prospectively, to protect the information, and retrospectively, in the event of an allegation of a violation of the protective order. The value, type and complexity of the information in this case warrant the protection of the patent bar. The bar eases both the expert's and the court's evaluation of what use of information or what activities are permitted. Revising the Order to impose only a use limitation, as suggested by Defendant, will likely lead to protracted and difficult disputes over possible indirect use of or benefit from the information. In addition, the Court notes that patent bars are not uncommon in cases involving valuable highly complex technical information.

Id. (footnotes omitted).

Although a patent prosecution bar may be necessary and right, hiring an outside expert might be complicated by the need to find one willing to forgo patent prosecution in the relevant area.

V. Conclusion

I have tried to avoid talking in absolutes because each trade secret case is different from the next. I hope, however, that I have suggested some options that can make your next trade secret investigation more navigable. In short:

- To cull the mass of information that the defendant stole down to a manageable and comprehendible core, ask the victim where the magic happens.
- If the purported trade secret seems open to debate, consider whether prosecution is warranted or whether to charge something other than theft of trade secrets, such as mail or wire fraud, or interstate transportation of stolen property.
- Consult with the victim early on about whether a patent prosecution bar will be necessary, because insisting upon one can affect whether outside experts will sign on to the prosecution and defense teams, and the briefing will be relatively novel for a criminal case.
- Consider whether your experts should include an outside expert, the victim's employees, or, in the right case, employees of the victim's competitors.
- If you use company employees as your experts, interview employees at various levels and divisions within the company to get the fullest picture of where the magic happens and whether the magic trick has been kept secret.
- Working with redacted trade secret exhibits might ease the process of working with defense experts and employees of the victim's competitors. ❖

ABOUT THE AUTHOR

❑ **Scott L. Garland** is an Assistant U.S. Attorney in the Anti-Terrorism and National Security Unit of the U.S. Attorney's Office for the District of Massachusetts. He started working on criminal trade secret investigations while in private practice. He continued focusing on them at the U.S. Department of Justice's Computer Crime and Intellectual Property Section from 2002 through 2008, where he served as a Trial Attorney, then a Senior Counsel, and was chief editor of the Section's *Prosecuting Intellectual Property Crimes* 2006 edition, and then at the U.S. Attorney's Office in Massachusetts, where he started in 2008 in the Office's Cybercrime Unit. In addition to other trade secret cases, Mr. Garland served as co-counsel in *United States v. Elliot Doxer*, which convicted a Massachusetts man for providing stolen trade secrets to an undercover federal agent posing as a foreign intelligence officer, and was only the eighth prosecution for foreign economic espionage in the nation. ✠

Child Pornography Conspiracies in the Digital Age: A Primer

Sarah Chang
Trial Attorney
Child Exploitation and Obscenity Section
Criminal Division

Keith Becker
Trial Attorney
Child Exploitation and Obscenity Section
Criminal Division

I. Introduction

As offenders become more sophisticated in their use of technology to produce, access, and obtain child pornography, they often seek out other like-minded individuals with whom to trade child pornography images and videos and discuss matters pertinent to the sexual exploitation of children. Internet technologies used by such offenders mirror those used by everyday Internet users—email, social networking Web sites, bulletin boards, peer-to-peer networks, Internet chat, and the like. The fact that offenders commit child pornography crimes together with others may present avenues for the collective prosecution of offenders using conspiracy statutes. However, offenders' use of certain technologies (for example, an email listserv where members send child pornography images out to a group of recipients, a social networking site where members join a private group to which they may upload child pornography, or a peer-to-peer network where members share folders of child pornography with certain trusted members) can create important legal issues related to the potential existence of multiple conspiracies. This article discusses legal issues pertinent to the prosecution of child pornography-related conspiracies with a focus on the issue of single versus multiple conspiracies.

II. A single agreement's evolution

Courts have long held that the "gist of the crime of conspiracy . . . is the agreement or confederation of the conspirators to commit one or more unlawful acts." *Braverman v. United States*, 317 U.S. 49, 53 (1942). "Whether the object of a single agreement is to commit one or many crimes, it is in either case that agreement which constitutes the conspiracy which the statute punishes." *Id.* Thus, "[t]he one agreement cannot be taken to be several agreements and hence several conspiracies because it envisages the violation of several statutes rather than one." *Id.* In *Braverman*, the Government charged the defendants with seven counts, each charging a conspiracy to violate separate and distinct internal revenue laws. The Government argued that if the jury found that a conspiracy existed, it must find the defendants guilty of as many offenses as it had illegal objects. Despite the trial judge's submission of the case to the jury on that theory, the jury returned a general verdict and found the defendants "guilty as charged." *Id.* at 51. The court sentenced each defendant to eight years' imprisonment. Upon review, the Supreme Court in *Braverman* agreed with the courts below that "however diverse its objects," a single agreement constitutes a single conspiracy. It affirmed the district court's decision to impose a single term of imprisonment as opposed to seven separate terms for each count of the indictment. *Id.* at 54.

While the *Braverman* Court did not address what constituted a "single agreement," the Supreme Court later built on that general principle of conspiracy law—that the essence of the crime is the

agreement to commit one or more unlawful acts—to define exactly how that agreement must be composed to constitute a single conspiracy. In 1946 and 1947, the Supreme Court considered two different conspiratorial schemes in *Kotteakos v. United States*, 328 U.S. 750 (1946), and *Blumenthal v. United States*, 332 U.S. 539 (1947), and provided some guidance on to how one might distinguish a single conspiracy from multiple conspiracies.

In *Kotteakos*, several individuals were convicted of conspiring to defraud the Federal Housing Administration by falsifying loan application documents, in violation of the National Housing Act (NHA). At trial, the Government showed that one of the conspirators, Simon Brown, acted as the common and key figure in all of the proven transactions by acting as a broker to place applications for NHA loans, purportedly for renovation and modernization projects, knowing that the loan proceeds would not be used for the purposes stated on the loan application. For example, one coconspirator asked Brown to obtain an NHA loan to finance a law firm, but directed Brown to state that the loan proceeds would be used to modernize a home. Though charged together as part of a single conspiracy, the defendants had no relationship to one another "other than that Brown had been the instrument in each instance for obtaining the loans." *Kotteakos*, 328 U.S. at 754. Borrowing from a turn of phrase offered by the Government, the Court noted that the charged conspiracy could be likened to "separate spokes meeting at a common center." *Id.* at 755 (internal quotation marks omitted). However, the Court added, "without the rim of the wheel to enclose the spokes," a single conspiracy could not be found. *Id.* As the Court observed, "[t]hieves who dispose of their loot to a single receiver—a single 'fence'—do not by that fact alone become confederates: they may, but it takes more than knowledge that he is a 'fence' to make them such." *Id.*

What "more" is required to prove a single conspiracy was addressed a year later in *Blumenthal*. In this case, the Government charged five individuals with a single conspiracy in a single count, alleging that they had conspired to dispose of two carloads (about 2,000 cases) of Old Mr. Boston Rocking Chair Whiskey at over the ceiling wholesale prices, in violation of federal law. According to the Government's proof at trial, the petitioners were middlemen who arranged the sales and deliveries of price-fixed whiskey to tavern owners from an unidentified, central distributor. While two of the petitioners, Goldsmith and Weiss, knew of one another's existence and role in the scheme (Goldsmith controlled the funds in the distributor's bank account, and Weiss acted as the sales manager), the other three, Feigenbaum, Blumenthal, and Abel, were seemingly unrelated "except that each had part in arranging sales and deliveries of portions of these two shipments to purchasers." *Blumenthal*, 332 U.S. at 544. However, the Court found convincing the following evidence to infer that Feigenbaum, Blumenthal, and Abel "were aware that their individual sales were part of a larger common enterprise": (1) almost simultaneously, the three salesmen made it known to tavern keepers that they could obtain whiskey for sale, (2) all three gave similar predictions to purchasers about when the whiskey would arrive, and (3) all three followed a "singularly set pattern in making their respective sales" (that is, they charged the identical price of $24.50 per case by check). *Id.* at 553 n.14.

A "hypertechnical" analysis of the scheme, the Court stated, would show that two separate agreements had formed: an agreement among Goldsmith, Weiss, and the unknown owner, and a second agreement among the five petitioners to which the unknown owner was not a party. *Id.* at 556. However, recognizing that conspiracies "are not born full grown" and "mature by successive stages," the Court held that the "two agreements were merely steps in the formation of the larger and ultimate more general conspiracy." *Id.* at 556–57. The difference between *Blumenthal* and *Kotteakos*, the Court explained, lies in the absence of any composition or evolution in the individual agreements found in *Kotteakos*: "[N]o two of those agreements were tied together as stages in the formation of a large all-inclusive combination, all directed to achieving a single unlawful end or result." *Id.* at 558. Each loan in *Kotteakos* was "an end in itself, separate from all others," whereas each whiskey transaction in *Blumenthal* built upon and depended on the other as part of a "single, over-all, comprehensive plan." *Id.* After all, each salesman in *Blumenthal* "knew the lot to be sold was larger and thus that he was aiding in a larger plan." *Id.* at 559.

"By their separate agreements . . . they became parties to the larger common plan, joined together by their knowledge of its essential features and broad scope, though not of its exact limits, and by their common single goal." *Id.* at 558.

Since then, appellate courts have further developed these principles to look beyond individual agreements to examine instead whether those agreements comprise a "collective venture directed toward a common goal" to determine the existence of a single conspiracy. *United States v. Berger*, 224 F.3d 107, 114 (2d Cir. 2000) (quoting *United States v. Maldonado-Rivera*, 922 F.2d 934, 963 (2d Cir. 1990)) (finding a single conspiracy where one overriding goal existed that was led by the same core group of community leaders and shared common participants who used the same distinctive methods and means in their different frauds, which were mutually interdependent). A single conspiracy can be shown by "one overall agreement," which "depends upon the overlap of key actors, methods, and goals." *United States v. Leavis*, 853 F.2d 215, 218 (4th Cir. 1988) (internal citations omitted) (finding a single conspiracy even over the course of two cocaine importation attempts because key actors had organized both attempts, operations were headquartered in the same beach house on both occasions, and the methods and goals remained the same throughout).

Among the different factors specified by each circuit, one factor is common: the existence of an agreement towards a common goal. *See United States v. Gilbert*, 721 F.3d 1000, 1005 (8th Cir. 2013) ("A single conspiracy may be found when the defendants share a common overall goal . . . ."); *United States v. Diaz-Arias*, 717 F.3d 1, 21 (1st Cir. 2013) (holding that there was sufficient evidence for the jury to determine that a single conspiracy existed based on the following factors: "(1) the existence of a common goal, (2) interdependence among participants, and (3) overlap among the participants"); *United States v. Acosta-Gallardo*, 656 F.3d 1109, 1124 (10th Cir. 2011) ("To make a finding of a single conspiracy, the jury must be convinced beyond a reasonable doubt that the alleged coconspirators possessed a common, illicit goal."); *United States v. Green*, 648 F.3d 569, 579 (7th Cir. 2011) ("A single conspiracy exists if the co-conspirators joined to effectuate a common design or purpose with the focus of the court's inquiry on that common purpose.") (internal citations omitted); *United States v. Brockenborrugh*, 575 F.3d 726, 737 (D.C. Cir. 2009) ("Whether a course of conduct should be classified as a single conspiracy or divided into multiple conspiracies depends on whether the participants shared a common goal, were dependent upon one another, and were involved together in carrying out at least some parts of the plan."); *United States v. Seher*, 562 F.3d 1344, 1366 (11th Cir. 2009) ("To determine whether the jury could have found a single conspiracy, we consider: (1) whether a common goal existed; (2) the nature of the underlying scheme; and (3) the overlap of participants."); *United States v. Smith*, 320 F.3d 647, 652 (6th Cir. 2003) ("The principal considerations in determining the number of conspiracies are the existence of a common goal, the nature of the scheme, and the overlapping of the participants in various dealings."); *United States v. Duran*, 189 F.3d 1071, 1080 (9th Cir. 1999) ("A single conspiracy can only be demonstrated by proof that an overall agreement existed among the conspirators.") (internal citations omitted); *United States v. Kelly*, 892 F.2d 255, 259 (3d Cir. 1989) (employing a three-step inquiry to determine whether a series of events constitutes a single conspiracy, which included an examination of whether there was a "common goal among the conspirators"); *United States v. Richerson*, 833 F.2d 1147, 1153 (5th Cir. 1987) ("In counting the number of conspiracies, the principal factors are (1) the existence of a common goal, (2) the nature of the scheme and (3) overlapping of participants in the various dealings."). The common goal can be as broad as "sell[ing] cocaine for profit or to further the distribution of cocaine." *Diaz-Arias*, 717 F.3d at 21. *See also United States v. Brito*, 721 F.2d 743, 747 (11th Cir. 1983) (finding a single conspiracy where conspirators held the common objective of importing marijuana into the U.S.).

III. Finding the common goal agreement in child pornography consumers, distributors, and producers

A. Commercial Web sites: buyers and sellers

The nature of commercial child pornography Web sites is simple: cash or monetary credit in exchange for images and videos of child pornography. While one could argue that a buyer on a commercial child pornography Web site shares a common goal with the seller—to further the trade of child pornography—it may be difficult to convincingly establish that there existed a separate agreement to further that goal outside the actual sale itself.

"It is well-settled that a simple buyer-seller relationship, without any prior or contemporaneous understanding beyond the sales agreement itself, is insufficient to establish that the buyer was a member of the seller's conspiracy." *United States v. Gibbs*, 190 F.3d 188, 197 (3d Cir. 1999); *see also United States v. Brown*, 726 F.3d 993, 998 (7th Cir. 2013) ("[While] the substantive trafficking crime is an agreement, it cannot also count as the agreement needed to find conspiracy.").

Finding evidence of such an agreement, that is, an agreement beyond the sales agreement between the buyer and seller, may be challenging in the commercial child pornography Web site context. As the Sixth Circuit reasoned in *United States v. Blakley*, 239 F. App'x 229, 235 (6th Cir. 2007) (unpublished opinion), the "mere act of buying child pornography for personal possession would not be a sufficient basis, standing alone, upon which to sustain a conspiracy conviction." In *Blakley*, we find facts that are familiar: a defendant's child pornography collection, discovered by his wife, is reported to law enforcement officials who then find various CD's and computer disks containing sexually explicit photographs of children, some of which are labeled with Web banners (an Internet address indicating that the picture had been downloaded from that particular Web site). When asked at oral argument to identify a coconspirator with whom an agreement had been reached in *Blakley*, the Government posited that the defendant had "conspired with unknown persons who had uploaded the images onto the various websites from which the defendant had then downloaded them." *Id.* at 234–35. The Sixth Circuit was not convinced. "[T]he record in this case is devoid of any evidence tending to establish that the defendant reached an agreement with any third party concerning the receipt or distribution of child pornography by computer or otherwise." *Id.* at 234.

While a conspiracy involving buyers of child pornography on a commercial Web site may be unlikely, the operators of such a Web site may be ripe for conspiracy charges. Individuals who jointly set up and maintain such a commercial Web site (securing computer server space, acquiring or producing child pornography to be sold, providing access to buyers, and collecting payments) may qualify for charges involving conspiracies to advertise or distribute child pornography or money laundering. A ready example is found in *United States v. Richards*, 659 F.3d 527 (6th Cir. 2011). The *Richards* court upheld convictions for conspiracy to distribute child pornography, as well as substantive counts of production, advertising, distribution, and possession of child pornography, and record-keeping violations. *Id.* at 536. The defendant in that case, Timothy Richards, operated at least a dozen Web sites that contained child pornography and advertisements for or links to other child pornography sites, including billing sites. Richards also managed and operated other pornography-related Web sites, including billing sites, profiting "handsomely" from a business that offered discounts for customers who visited multiple sites, standard and premium membership plans, and online credit card processing for membership payments. *Id.* at 531. Not only did Richards personally produce child pornography, but he, along with coconspirators, secured and operated computer servers in his home and elsewhere that hosted the Web sites and the associated child pornography.

B. Peer-to-peer networks

Proving an agreement to accomplish a common goal will be difficult in a peer-to-peer context. Like each loan in *Kotteakos*, each peer-to-peer transaction can be "an end in itself," *Blumenthal*, 332 U.S. at 558 (explaining *Kotteakos*). Unlike the hub and spoke model, a peer-to-peer network is usually a decentralized network in which individuals, "peers," both supply and consume one another's resources. And unlike the chain model discussed by the Supreme Court in *Blumenthal*, where each link contributes to the conspiracy's ultimate goal, a peer-to-peer network can seemingly have multiple goals and multi-faceted links that do not culminate into one comprehensive plan. When neither wheel nor chain models are helpful, courts return to the basic building block of conspiracy, the agreement, and ask, "[W]hat is the nature of the agreement?" *United States v. Brito*, 721 F.2d 743, 747 (11th Cir. 1983). Those who seek to charge multiple peer-to-peer network users in a single conspiracy should proceed with caution and ensure that the decentralized nature of the peer-to-peer network does not defeat the existence of a single agreement.

There is some precedent, however, for charging a conspiracy when the moderators or administrators of peer-to-peer networks engage in criminal activity, just as with the owners, operators, and administrators of commercial child pornography Web sites. In 2005, William Trowbridge and Michael Chicoine each pleaded guilty to one count of conspiracy to commit felony criminal copyright infringement, in violation of 18 U.S.C. § 371. Their convictions were the first federal convictions for copyright piracy using peer-to-peer networks. *See* Press Release, U.S. Department of Justice, First Criminal Defendants Plead Guilty in Peer-To-Peer Copyright Piracy Crackdown, *available at* http://www.justice.gov/opa/pr/2005/January/05_crm_022.htm. According to the Government's sentencing memorandum, Trowbridge and Chicoine each owned, operated, and moderated a hub via a peer-to-peer file sharing software called Direct Connect on the Underground Network, an organized group of Direct Connect hub operators. *See* Government's Motion for Downward Departure and Memorandum in Aid of Sentencing, Crim. No. CR-04-552-01 (PLF), 1–3 (filed Sept. 6, 2005) (hereinafter Trowbridge Memorandum). *See also* Government's Memorandum in Aid of Sentencing, Crim. No. CR-04-553-01 (PLF), 1–3 (filed Sept. 6, 2005) (hereinafter Chicoine Memorandum). A "hub" is a "feature of Direct Connect networks similar in theory to a room where users congregate." Trowbridge Memorandum, at 3. At a hub, one could also browse an index of all the files being shared by each user connected to a particular hub. A hub can also function like a user or member connected to the hub and share files itself. *See id.* To access the Underground Network, one connected to the Internet activated the Direct Connect software, visited the Web site www.udgnet.com, and signed up for membership. *See id.* No fee attached with registration, and upon registration, one could access a list of hub sites on the Underground Network, browse or search directories of files shared by a "peer," and use the private and shared messaging functions offered by the network. A hub operator is generally the owner of a hub and may double as the moderator. A hub operator independently establishes rules for membership and use and enforces them by controlling access to the hub and the content of files shared through the hub. A moderator monitors and regulates the hub.

Three years later, the first peer-to-peer copyright infringement case to go to trial resulted in a guilty verdict in the Western District of Virginia. *See* Press Release, U.S. Department of Justice, Federal Jury Convicts High Ranking Web Site Administrator in Peer-to-Peer Piracy Crackdown, *available at* http://www.justice.gov/opa/pr/2008/June/08-crm-574.html; *see also* Indictment, *United States v. Dove*, No. 2:07CR15, 2007 WL 6065066 (W.D.V.A. Aug. 28, 2007). The Government's indictment alleged that Dove, an administrator and a member who uploaded content to Elite Torrents (a peer-to-peer network that used BitTorrent technology), conspired with others to infringe copyrights by reproducing and distributing copyrighted works. *Id.* Elite Torrents differed from Direct Connect in that instead of hubs, there was a "tracker" server that kept track of, among other things, logged-in members and the contents of their file directories available for upload. There was also an explicit "price" for membership. Elite Torrents required members to upload at least as much pirated content as they downloaded to remain members.

When a member violated these rules, an Administrator could access the tracker and demote or ban the offending member. *Id.*

C. Bulletin boards

Internet bulletin boards dedicated to child pornography have provided a strong predicate for conspiracy charges in child pornography cases. Several examples of such conspiracies are discussed in the context of the child exploitation enterprise statute, 18 U.S.C. § 2252A(g), in the July 2013 United States Attorneys' Bulletin article by Keith Becker and John "Luke" Walker, titled *Conspiracy and Internet Technology: Using the Child Exploitation Enterprise Statute to Prosecute Online Child Exploitation*. Such criminal organizations, often consisting of hundreds of members, share numerous characteristics that make them amenable to prosecution as a single overarching conspiracy, such as: membership requirements and rules, often including a requirement to post child pornography to obtain membership and continue posting child pornography to remain a member; division of responsibilities among members, such as administering the group, compiling postings for all members, or soliciting and facilitating payments for server space or producers of new child pornography images; security consciousness, including member postings giving advice about how to avoid law enforcement detection through use of proxies and encryption technologies; and graduated membership levels allowing greater access to more material based upon active participation. Such characteristics provide evidence of the "trust, cooperation, and delineation of duties among participants in a common scheme" that indicates the existence of a single conspiracy. *United States v. Green*, 648 F.3d 569, 579 (7th Cir. 2011) (citing *United States v. Handlin*, 366 F.3d 584, 590 (7th Cir. 2004)).

D. Email distribution lists

There is also precedent for charging members of a child pornography email distribution list within a conspiracy. In January 2012, nine defendants were charged in the Western District of Virginia with conspiracy to distribute, receive, and possess or access with intent to view child pornography pursuant to 18 U.S.C. § 2252(a)(2), (a)(4)(B), (b)(1), and (b)(2), for their participation in such an email distribution list. *United States v. Allen*, No. 6:12-cr-00002-8, 2012 WL 1833889, at *1 (W.D. Va. May 18, 2012). Eight of those nine defendants were successfully prosecuted either in the Western District of Virginia or other federal jurisdictions. The ninth defendant, known as "Andy Danilov," who distributed emails to the list, is believed to reside in Russia and remains at large.

In April 2011, the FBI executed a search warrant on an email account (distributor account), which revealed that the account holder had sent large amounts of child pornography to more than 50 other email accounts on a regular basis over a period of nearly 5 years. The distributor account was the main distributor of emails containing links to sequentially numbered compressed files, as well as file attachments, depicting minors engaged in sexually explicit conduct. Review of the distributor account further disclosed that members were added to the email group after finding contact information for the account holder on Web sites that depicted child erotica and child pornography, or after communicating shared interests on social media networking Web sites. Once a person was added to the group, he or she would receive emails that contained links to sequentially numbered compressed files or file attachments depicting minors engaged in sexually explicit conduct.

Importantly, once part of the group, all of the charged members were given the opportunity to withdraw. For instance, during the course of the conspiracy, the account holder sent to charged members of the group an email message specifically asking members whether they wished "To stop mailing, or—To continue mailing." *Id.* at *2. In response, defendants who were ultimately charged with conspiracy either replied by email indicating that they wanted to continue receiving emails or did not respond to the email but also did not request to be removed from the email group. All of those charged continued to receive emails from the distributor account. Forensic examinations of all charged defendants' computers,

in addition to information derived from defendant interviews, confirmed each defendant's participation in the conspiracy and revealed emails containing child pornography received from the distributor account and/or evidence detailing how a particular defendant encountered Danilov online and went about joining the email distribution list. The agreement to form a conspiracy, the Government argued, was established in each charged member's response to the invitation to withdraw or continue their membership.

Earlier, in *United States v. Froman*, 355 F.3d 882 (5th Cir. 2004), the Fifth Circuit reviewed a conspiracy conviction for a defendant who had participated in an "e-group" for child pornography called "Candyman E-Group." *Id.* at 884. Candyman E-Group, a hybrid bulletin board/email distribution group, allowed members to post images or video files for other members to view and download. When a member uploaded content to the Candyman E-Group Web site, all subscribers would receive an email, daily digest notification, or no email and would simply review the content on the Web site where they were archived. In his appellate brief, Froman argued that fruits of a contested search ought to have been suppressed and that without these evidentiary fruits his conspiracy conviction could not stand. *See id.* at 884, 891. He did concede, however, that if the motion to suppress was denied, there was sufficient evidence for conviction. *Id.* at 891. The Fifth Circuit affirmed the district court's probable cause finding and, in combination with Froman's concession, also affirmed his conviction. *Id.* Though it did not specifically address the elements of conspiracy, the Fifth Circuit detailed the facts of the case and highlighted the following: that the main Web page for the group announced its mission ("This group is for People who love kids. You can post any type of messages you like too [sic] or any type of pics and vids you like too [sic]." *Id.* at 885.); that in order to access the Web site and all its functions (including an email distribution list), one needed to subscribe; and that Froman had subscribed to be a member of the group and continued to subscribe to the group until it was shut down a month later. *Id.* Though it is unclear whether Froman had opted out of the email distribution list, the court's review of the facts evidences its search for an agreement and a common goal. *Id.* at 890–91.

IV. Conclusion

The varying technologies used by offenders to produce, distribute, and obtain child pornography materials present numerous avenues of collective prosecution. When contemplating a single conspiracy charge, prosecutors are urged to make sure that the individual agreements formed amongst coconspirators lead to or manifest a common objective. ❖

ABOUT THE AUTHORS

❑ **Sarah Chang** has been a trial attorney with the Department of Justice, Criminal Division, Child Exploitation and Obscenity Section since 2012. From 2009 to 2012, she was a trial attorney with the Criminal Division's Human Rights and Special Prosecutions Section, where she prosecuted international violent crimes, alien smuggling, and identity theft offenses. She also served as a Special Assistant U.S. Attorney with the U.S. Attorney's Office for the District of Columbia, where she prosecuted local cases involving domestic violence and sex abuse. ✠

❑ **Keith Becker** has been a trial attorney with the Department of Justice, Criminal Division, Child Exploitation and Obscenity Section since 2010. He served as co-counsel in the prosecution of the Dreamboard online child pornography forum, the largest U.S. prosecution to date of individuals who participated in an online bulletin board dedicated to promoting child sexual abuse and disseminating child pornography. From 2005 to 2010, he was an Assistant U.S. Attorney for the District of Columbia, where he prosecuted federal and local cases involving violent crime, narcotics, and child pornography. ✠