Caution Advised: Avoid Undermining the Legitimate Needs of Law Enforcement to Solve Crimes Involving the Internet in Amending the Electronic Communications Privacy Act

By KEVIN V. RYAN AND MARK L. KROTOSKI*

Introduction

MANY CRIMES TODAY ARE COMMITTED on the Internet. With each year, new Internet avenues, channels and tools become available. New applications are popular on mobile devices that were unavailable only a few years ago. The Internet continues to offer a broadening and varied opportunity to communicate and access information.

While the Internet has resulted in many positive benefits for society, it also offers unique advantages to criminals to exploit victims. The Internet provides the means to communicate with or access computers around the world in real-time, twenty-four hours a day seven

* Honorable Kevin V. Ryan, Adjunct Professor of the University of San Francisco Law School. Mr. Ryan previously served as U.S. Attorney in the Northern District of California where, among other duties, he supervised the Computer Hacking and Intellectual Property ("CHIP") Unit based in Silicon Valley. Mr. Ryan previously was a Municipal and Presiding Superior Court Judge in the County of San Francisco, Director of the San Francisco Mayor's Office of Criminal Justice and a Deputy Chief of Staff to the Mayor, a Deputy District Attorney in Alameda County and a litigation partner in a notable law firm.

Mark L. Krotoski, a federal prosecutor since 1995, served as Criminal Division Chief in the U.S. Attorney's Office in the Northern District of California and as a CHIP Prosecutor in Silicon Valley and in the Eastern District of California. Among other positions, for nearly four years, Mr. Krotoski served as National CHIP Program Coordinator at the Computer Crime and Intellectual Property Section in the Criminal Division of the U.S. Department of Justice. He has prosecuted and supervised a wide variety of computer intrusions, theft of trade secrets, economic espionage, criminal copyright and trademark violations, computer fraud, click-fraud, and other Internet-based and fraud crimes.

The views expressed are those of the authors and do not necessarily reflect the views of the U.S. Department of Justice. The authors wish to express their appreciation for the review and constructive comments on earlier drafts of this article, including Josh Goldfoot and Jason Passwaters, among others.

days a week. Taking advantage of the global reach of the Internet, perpetrators may be many time zones away in another jurisdiction or country. Perpetrators can even be in the same neighborhood as the victim but may have redirected their Internet transmissions to make it appear that they are in another country. The Internet provides unique levels of anonymity as well.[1] Active steps to conceal criminal activity on the Internet may have been taken (such as using a public library computer, using a proxy or "bouncing" through multiple locations).[2] The perpetrator may have taken steps to frame someone else.[3] Key records may have been transferred or deleted after the investigation became known, complicating the process to recover this evidence. Malware can be used to exploit and damage a computer or network and to collect banking information for fraud transactions.[4]

This Article seeks to provide a better understanding about the process that law enforcement uses to obtain Internet records under the Electronic Communications Privacy Act of 1986, as amended ("ECPA").[5] The process to identify, preserve, request, and obtain Internet evidence can be cumbersome, involving many steps and subject to numerous delays.[6] Because Internet records are retained for a lim-

1. As one example of the anonymity afforded on the Internet to commit crime, in a "vishing," or voice phishing scheme, "criminals can take advantage of cheap, anonymous Internet calling available by using Voice over Internet Protocol ("VoIP"), which also allows the criminal to use simple software programs to set up a professional sounding automated customer service line, such as the ones used in most large firms." The perpetrator, offering an aura of legitimacy, "emulates a typical bank protocol in which banks encourage clients to call and authenticate information." BINATIONAL WORKING GROUP ON CROSS-BORDER MASS MARKETING FRAUD, REPORT ON PHISHING: A REPORT TO THE MINISTER OF PUBLIC SAFETY AND EMERGENCY PREPAREDNESS CANADA AND THE ATTORNEY GENERAL OF THE UNITED STATES 10 (2006) [hereinafter REPORT ON PHISHING], *available at* http://www.justice.gov/opa/ report_on_phishing.pdf; *see also infra* note 15 (providing a definition of "vishing").

2. *See infra* note 121 and Part II.D.

3. *See infra* note 83.

4. "Malware" is "[a] program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim." NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, GLOSSARY OF KEY INFORMATION SECURITY TERMS 115 (Richard Kissel ed., 2011) [hereinafter GLOSSARY OF SECURITY TERMS], *available at* http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf; *see also* ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, MALICIOUS SOFTWARE (MALWARE): A SECURITY THREAT TO THE INTERNET ECONOMY: MINISTERIAL BACKGROUND REPORT 10 (2007) [hereinafter MALWARE REPORT], *available at* http://www.oecd.org/dataoecd/53/34/40724457.pdf (describing malware as "a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners[.]").

5. For more on ECPA see *infra* notes 44–48.

6. The ten steps are described below. *See infra* Part II.C.

ited period, from only a few days to a couple months or more, law enforcement normally is racing to obtain them as new leads are provided.

The ability of law enforcement to obtain these records impacts at least six public policy and criminal justice interests, including: (1) promoting confidence in the use of the Internet; (2) addressing the legitimate needs of law enforcement to investigate and prosecute crimes committed over the Internet; (3) addressing the rights and interests of crime victims; (4) attaining the public policy objectives identified by Congress in enacting a particular criminal statute; (5) providing a fair process, ensuring that the responsible perpetrators are identified and fairly prosecuted; and (6) balancing and respecting privacy interests.

Recent debate and legislation has suggested that the law by which law enforcement obtains Internet records may be changed. Any proposal that modifies current processes should explicitly answer the question about how much longer law enforcement would be delayed in obtaining Internet records under the new standards. If more delay will result, retention standards should be imposed to ensure that the Internet trail of evidence will be available upon sufficient legal process. Retention standards apply to other information, including medical, financial and employment records.[7]

A. Examples of Crimes Involving the Internet

There are many crimes that may be committed either entirely or at least partially on the Internet. This includes Internet-based crimes as well as traditional crimes such as murders, violent crimes, kidnappings, and other offenses, in which Internet records have been created that are related to the crime and may help solve it. Some cybercrimes also impact national security and critical infrastructure concerns.

1. Internet-Based Crimes

According to one recent report, numerous common Internet crimes are based in fraud such as identity theft, advance fee fraud, non-auction/non-delivery of merchandise, and overpayment fraud.[8] According to the recent 2012 Verizon Data Breach Report, most data breaches were accomplished by hacking (81% of breaches, compro-

7. *See infra* Part IV.D.2 (discussing retention periods for certain health, banking and employment records).

8. *See* INTERNET CRIME COMPLAINT CENTER, 2011 INTERNET CRIME REPORT 10 (2012), *available at* http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf.

mising 99% of records) or the use of malware (69% of breaches, 95% of records).[9]

Internet-based crimes take many forms. For example, some common offenses may include: computer intrusions or unauthorized computer access;[10] identity theft and aggravated identity theft;[11] credit card or bank fraud;[12] "phishing";[13] "spearphishing";[14] "vishing";[15]

9. VERIZON COMMC'NS, INC., 2012 DATA BREACH INVESTIGATIONS REPORT 26, 30 (2012), *available at* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf (reviewing 855 incidents resulting in 174 million compromised records which includes a study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit, and United States Secret Service).

10. Unauthorized access to computers including hacking offenses are normally prosecuted under 18 U.S.C. § 1030 (2011) (fraud and related activity in connection with computers). There are numerous examples of hacking prosecutions under section 1030(a). *See, e.g.*, United States v. Heckenkamp, 482 F.3d 1142, 1143–46 (9th Cir. 2007) (affirming conviction of computer science student for hacking into a computer system of Qualcomm Corporation in San Diego from computers at the University of Wisconsin); United States v. Trotter, 478 F.3d 918, 919–22 (8th Cir. 2007) (affirming section 1030(a)(5) conviction for hacking into the Salvation Army computer network and deleting files, shutting down a computer-operated telephone system and other disruptive conduct); United States v. Phillips, 477 F. 3d 215, 218 (5th Cir. 2007) (affirming conviction under section 1030(a)(5) for launching a brute-force attack program on a university system over 14 months to obtain personal information and Social Security numbers on "more than 45,000 current and prospective students, donors, and alumni"); United States v. Ivanov, 175 F. Supp. 2d 367, 367–70 (D. Conn. 2001) (denying motion to dismiss indictment based on unauthorized access by defendant in Russia to computer servers in Connecticut).

11. Identity theft and aggravated identity theft are prosecuted under 18 U.S.C. §§ 1028 (fraud and related activity in connection with identification documents, authentication features, and information), and 1028A (aggravated identity theft) respectively. *See, e.g.*, Judgment, United States v. Adegoke, No. 1:10-cr-00103-LO (E.D. Va. Oct. 22, 2010), ECF No. 29 (defendant sentenced to 102 months in prison and ordered to pay $696,026 in restitution following his wire fraud and aggravated identity theft convictions in an airline ticket fraud scheme using email accounts and VOIP); Judgment, United States v. Craig, No. 08-CR215 (S.D. Tex. Apr. 29, 2009), ECF No. 33 (defendant sentenced to 72 months in prison after compromising the personal data of more than 17,000 active duty and reserve military personnel, including their social security numbers, names, and computer-use profiles, which he attempted to sell to a person he believed was a foreign agent of the People's Republic of China); Press Release, U.S. Dep't of Justice, Nigerian National Sentenced to 102 Months in Prison for Role in Airline Ticket Scam (Oct. 22, 2010), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2010/ adegokeSent.pdf; Press Release, U.S. Dep't of Justice, Military Computer Contractor Pleads To Unauthorized Access To Military Database and ID Theft (May 2, 2008), *available at* http:// www.justice.gov/ criminal/cybercrime/press-releases/2008/craigPlea.pdf.

12. Credit card fraud may be prosecuted under 18 U.S.C. §§ 1029 (fraud and related activity in connection with access devices) and 1344 (bank fraud). Under section 1029(e), an "access device" includes "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). Other legal theories of criminal liability for these acts, depending on the facts of the case include 18 U.S.C. §§ 1343 (fraud by wire, radio, or television) and 1341 (frauds and swindles—mail fraud). *See, e.g.*, United States v. Drummond, 255 F. App'x 60 (6th Cir. 2007) (affirming jury trial conviction for wire fraud and possession of fifteen or more credit card numbers with the intent to defraud for fraudulent online airline reservation using the identity of another individual made while the defendant was on supervised release for an earlier credit card fraud conviction).

13. "Phishing" generally refers to

> [T]he creation and use by criminals of e-mails and websites—designed to look like they come from well-known, legitimate and trusted businesses, financial institutions and government agencies—in an attempt to gather personal, financial and sensitive information. These criminals deceive Internet users into disclosing their bank and financial information or other personal data such as usernames and passwords, or into unwittingly downloading malicious computer code onto their computers that can allow the criminals subsequent access to those computers or the users' financial accounts.

REPORT ON PHISHING, *supra* note 1, at 4 (footnote omitted); *see also* GLOSSARY OF SECURITY TERMS, *supra* note 4, at 138 (defining phishing as "[t]ricking individuals into disclosing sensitive personal information through deceptive computer-based means").

Phishing cases are normally prosecuted under applicable fraud statutes, depending how the crime was committed, such as 18 U.S.C. §§ 1028, 1029, 1030, 1343. *See, e.g.*, United States v. Blount, 377 F. App'x 55, 57 (2d Cir. 2010) (affirming plea conviction and 48 month sentence for conspiracy to commit fraud in connection with access devices under section 1029(b)(2) as part of an Internet phishing fraud conspiracy involving more than 250 victims); *see also* Press Release, U.S. Dep't of Justice, West Haven Man Involved In Email Phishing and Spamming Scheme Sentenced to Four Years in Prison (Mar. 24, 2009), *available at* http://www.justice.gov/usao/ct/Press2009/20090324.html. One of the largest phishing prosecutions to date was prosecuted in the Central District of California, known as "Operation Phish Phry," in which nearly 100 persons were charged in the United States and Egypt. Under the scheme, "Egyptian-based hackers obtained bank account numbers and related personal identification information from an unknown number of bank customers through phishing" and involved participants in both countries. Press Release, U.S. Dep't of Justice, One Hundred Linked to International Computer Hacking Ring Charged by United States and Egypt in Operation Phish Phry (Oct. 7, 2009) [hereinafter Operation Phish Phry], *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2009/egyptoperationChar.pdf; *see also, e.g.*, *Blount*, 377 F. App'x at 57 (affirming 48 month sentence for "conspiracy to commit fraud in connection with access devices in violation of 18 U.S.C. § 1029(b)(2), for his role in an Internet 'phishing' fraud conspiracy that ensnared over 250 victims and resulted in losses of over $120,000"); United States v. Nguyen, No. 2:07-CR-0164 MCE (E.D. Cal.); Press Release, U.S. Dep't of Justice, Sacramento Man Charged With Computer Fraud and Aggravated Identity Theft, Internet 'Phishing' Scheme Used to Steal Thousands of Credit and Debit Card Numbers, Social Security Numbers (April 26, 2007), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2007/nguyenCharge.pdf; Robert McMillan, *Phisher Who Hit 38,500 Gets Long Prison Sentence*, COMPUTERWORLD (July 28, 2011), http://www.computerworld.com/s/article/9218732/Phisher_who_hit_38_500_gets_long_prison_sentence ("A California man was sentenced to 12 years and seven months in prison Thursday for his role as the brains behind a widespread phishing scam that took in more than 38,000 victims.").

14. "Spear phishing," which is a variant of phishing,

"scareware;"[16] "ransomware;"[17] trade secret theft and economic espionage,[18] criminal spamming;[19] the sexual exploitation of children;[20]

---

is a technique whereby e-mails that appear genuine are sent to all the employees or members within a certain company, government agency, organization, or group. Much like a standard phishing e-mail, the message might look like it comes from an employer, or from a colleague who might send an e-mail message to everyone in the company, in an attempt to gain login information. Spear phishing scams work to gain access to a company's entire computer system.

REPORT ON PHISHING, *supra* note 1, at 3.

15. "Vishing," another variant of phishing,

involves identity thieves sending an e-mail designed in the same way as a phishing e-mail, yet instead of providing a fraudulent link to click on, the e-mail provides a customer service number that the client must call and is then prompted to "log in" using account numbers and passwords. Alternately, consumers will be called directly and told that they must call a fraudulent customer service number immediately in order to protect their account.

REPORT ON PHISHING, *supra* note 1, at 3.

16. "Scareware" is defined as "malicious computer programs designed to trick a user into buying and downloading unnecessary and potentially dangerous software, such as fake antivirus protection[.]" *Scareware*, OXFORD DICTIONARIES, http://oxforddictionaries.com/definition/ english/scareware (last visited Jan 21, 2013); *see also, e.g.*, Press Release, U.S. Dep't of Justice, U.S. Indicts Ohio Man And Two Foreign Residents In Alleged Ukraine-Based "Scareware" Fraud Scheme That Caused $100 Million In Losses To Internet Victims Worldwide (May 27, 2010), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2010/sundinIndict.pdf; FRANÇOIS PAGET, MCAFEE, INC., RUNNING SCARED: FAKE SECURITY SOFTWARE RAKES IN MONEY AROUND THE WORLD (2010), *available at* http://www.mcafee.com/us/resources/white-papers/wp-running-scared-fake-security-software.pdf.

17. "Ransomware" is used to describe:

the type of malware that can infect a PC and then lock the user's data most commonly by encrypting files or by injecting a rogue MBR (master boot record) to the system's start-up routine. . . . While the user's files are typically locked until the ransom is paid, the victim is still free to browse the Internet, thus allowing the banking Trojan to continue collecting information on the victim uninterrupted.

EMC CORP., RANSOMWARE: INFECT ME NOT 1 (2012), *available at* http://www.rsa.com/solutions/consumer_authentication/intelreport/11733_Online_Fraud_report_0612.pdf; *see also* John E. Dunn, *Ransom Trojans Spreading Beyond Russian Heartland*, TECHWORLD (March 9, 2012), http://news.techworld.com/security/3343528/ransom-trojans-spreading-beyond-russian-heartland; *Intelligence Note: Citadel Malware Delivers Reveton Ransomware in Attempts to Extort Money*, INTERNET CRIME COMPLAINT CENTER (May 30, 2012), http:// www.ic3.gov/media/2012/120530.aspx (describing the ransomware as "an attempt to extort money with the additional possibility of the victim's computer being used to participate in online bank fraud").

18. Economic espionage and trade secret theft, involving the criminal misappropriation of trade secrets, are prosecuted under 18 U.S.C. §§ 1831–39. *See* Mark Krotoski, *Identifying and Using Electronic Evidence Early to Investigate and Prosecute Trade Secret and Economic Espionage Act Cases*, 57 U.S. ATT'YS BULL. 42, 43–46 (Nov. 2009) (providing examples of electronic evidence used in trade secret and economic espionage cases), *available at* http://www.justice.gov/usao/eousa/ foia_reading_room/usab5705.pdf [hereinafter *Electronic Evidence In EEA Cases*]. *United States v. Meng* provides an example of an economic espionage case involving email communications. *See* Plea Agreement, United States v. Meng, CR 04-20216 JF (N.D. Cal. Aug. 29, 2007); *infra* note 55 and accompanying text.

cyberstalking;[21] transmitting threatening communications on the internet;[22] distribution of unlawful materials; copyright infringement;[23]

19. Criminal spamming is prosecuted under the CAN-SPAM Act. Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act), Pub. L. No. 108-187, 117 Stat. 2699 (codified at 18 U.S.C. § 1037). There are numerous examples of CAN-SPAM Act prosecutions. *See, e.g.*, United States v. Kilbride, 584 F.3d 1240 (9th Cir. 2009) (affirming jury conviction for CAN-SPAM and related violations involving the operation of an International pornographic spamming business); Indictment, United States v. Ralsky, No. 2:07-cr-20627-MOB-RSW (E.D. Mich. Jan. 3, 2008), ECF No. 4 (eleven defendants charged with CAN-SPAM and related charges for multi-million dollar e-mail stock fraud scheme). *See generally* Press Release, U.S. Department of Justice, Detroit Spammer and Three Co-Conspirators Sentenced for Multi-Million Dollar E-Mail Stock Fraud Scheme, *available at* http://www.justice.gov/opa/pr/2009/ November/09-crm-1275.html (three defendants sentenced to 40 and 51 months in prison). SPAM is defined as the "abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages." GLOSSARY OF SECURITY TERMS, *supra* note 4, at 180.

20. Child sexual exploitation offenses may include 18 U.S.C. §§ 2251 (sexual exploitation of children including production of child pornography), 2251A (selling or buying of children), 2252 (possession, distribution and receipt of child pornography), 2252A (certain activities relating to material constituting or containing child pornography), 2260 (production of sexually explicit depictions of a minor for importation into the United States), 2241 (aggravated sexual abuse), 2242 (sexual abuse), 2243 (sexual abuse of a minor or ward), 2244 (abusive sexual contact). The Internet is often used as a vehicle to commit these offenses. *See, e.g.*, STAFF OF H. COMM. ON ENERGY & COMMERCE, 109TH CONG., REP. ON SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET (Comm. Print 2007) [hereinafter STAFF REPORT: SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET], *available at* http:// republicans.energycommerce.house.gov/108/News/01032007_Report.pdf ("Crimes involving the sexual exploitation of children over the Internet are a growing problem in the U.S. and around the world, due to the ease with which pedophiles and child predators can trade, sell, view, and download images of child pornography from the Internet."). Examples of child sexual exploitation cases that could not be solved based on the unavailability of provider records are treated below. *See infra* notes 56–57 and accompanying text.

21. Cyberstalking may be prosecuted under 18 U.S.C. § 2261A. *See, e.g.*, United States v. Rose, 315 F.3d 956, 957 (8th Cir. 2003) (affirming 120 month sentence for interstate stalking and threatening communications which included "threatening and vulgar e-mail and telephone messages" sent to the victim and her family).

22. Threatening communications transmitted over the Internet may be prosecuted under 18 U.S.C. § 875(c). *See, e.g.*, Irizarry v. United States, 553 U.S. 708, 710 (2008) (in considering sentencing issue, case involved section 875(c) conviction for sending "an e-mail threatening to kill his ex-wife and her new husband" and for sending 'dozens' of similar e-mails in violation of a restraining order"); United States v. Kammersell, 196 F.3d 1137, 1138 (10th Cir. 1999) (affirming section 875(c) conviction for transmitting a bomb threat via AOL "instant message"; interstate requirement applied to the transmission by the defendant to the recipient in the same state since the threatening communication was transmitted "traveled out of Utah to Virginia" where AOL servers were located "before returning to Utah").

23. Copyright infringement may be prosecuted under 18 U.S.C. § 2319. *See, e.g.*, United States v. Slater, 348 F.3d 666 (7th Cir. 2003) (affirming convictions and sentences for 24 and 8 months for two defendants convicted for to commit copyright infringement of copyrighted software over the Internet through a group known as "Pirates With Attitudes"); Criminal Minute Order, United States v. Fish, No. 5:06-cr-00109-RMW (N.D. Cal.

illegal wiretap;[24] and obstruction of justice (by deleting Internet records known to be within the scope of an investigation),[25] to name only a few.

2. Traditional Crimes Involving Internet Evidence

The use of Internet evidence is not limited to crimes committed exclusively or substantially on the Internet. The investigation and resolution of more traditional crimes may also rely on Internet evidence.

Murder cases have been solved by Internet or electronic evidence.[26] In one murder case, for example, text messages from the defendant's cell phone carrier provided key evidence. Normally, text messages are only retained for a few days. However, in this case, the records had unexpectedly been preserved. Along with other cell tower data, the text messages were "the single most important piece of evidence in linking the defendant to the" murders of a 22-year old and

May 9, 2008), ECF. No. 18 (defendant who served as a site operator, scripter, equipment supplier, broker and encoder for warez sites, distributing newly released movies, games, software and music online, was sentenced to 30 month in prison); Press Release, U.S. Dep't of Justice, Connecticut Man Sentenced To 30 Months In Prison For Criminal Copyright Infringement (Apr. 29, 2008), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2008/fishSent.pdf (noting that forty individuals were convicted during the investigation known as Operation Copycat and Operation Site Down).

24. An illegal interception may violate the Wiretap Act, under ECPA, Title I, 18 U.S.C. §§ 2510–22. *See, e.g.*, United States v. Szymuszkiewicz, 622 F.3d 701, 705 (7th Cir. 2010) (affirming section 2511 conviction for employee monitoring and intercepting email communications sent to his supervisor).

25. *See, e.g.*, United States v. Kernell, 667 F.3d 746, 749–50 (6th Cir. 2012) (affirming obstruction of justice trial conviction under 18 U.S.C. § 1519 for the deletion of computer information relating to unauthorized access to the email account of Alaska Governor and Vice Presidential candidate Sarah Palin); United States v. Smyth, 213 F. App'x 102, 102 (3d Cir. 2007) (defendant pled guilty to violating section 1519 for destroying a computer hard drive with intent to obstruct a federal investigation of child pornography); United States v. Fumo, 628 F. Supp. 2d 573, 599 (E.D. Pa. 2007) (affirming use of 18 U.S.C. § 1519 to conspiracy to "obstruct justice by destroying electronic evidence, including e-mail communications pertaining to matters within the scope of a federal criminal investigation").

26. *See, e.g.*, Monica Davey, *Computer Disk Led to Arrest in Killings, Pastor Says,* N.Y. TIMES (Mar. 2, 2005), http://www.nytimes.com/2005/03/02/national/02btk.html (in the "bind, torture, and kill" murders, information on the computer disk in the defendant's final mailing was used "to trace it back to a computer at Christ Lutheran Church" that the defendant "had used . . . a few weeks earlier"); Eli Ross, *Thursday Testimony in Baker Murder Trial Filled With Twists, Turns, Technical Talk,* KWTX.COM (Jan. 14, 2010), http://www.kwtx.com/home/headlines/ 81127767.html (in homicide of former minister's wife, originally ruled a suicide, the computer forensic trial testimony revealed the defendant had searched on the Internet for the phrase "overdose on sleeping pills"); Richard Williams, *Baby Video Torture Killer an 'Evil Monster.'* SKY NEWS ONLINE (Dec. 2, 2010), http://news.sky.com/skynews/Home/UK-News/Charlie-Hunt-Murderer-Of-Baby-Filmed-While-He-Was-Tortured-Darren-Newton-Branded-Evil-Monster/Article/201012115845372?f=rss (mobile phone used to video torture of baby who was murdered).

her 10-month old son.[27] Kidnappings and violent crimes have been resolved with cell site data from providers.[28]

In sum, any crime committed using the Internet, cell phones or other similar devices may have electronic evidence records that may be used to solve the crime. The ability to obtain this evidence, which may be essential to solving the crime, may turn on the availability of the Internet records.

3. National Security and Critical Infrastructure Concerns

The inability of law enforcement to obtain Internet records also has national security and critical infrastructure implications. Cyber attacks have been increasing exponentially. As the 2012 National Preparedness Report noted:

> Cyber attacks have increased significantly in number and sophistication in recent years, resulting in the Federal Government and private sector partners expanding their cybersecurity efforts. The U.S. Computer Emergency Readiness Team (US-CERT) reported an over 650-percent increase in the number of cyber incidents reported by federal agencies over a five-year period, from 5,503 in FY 2006, to 41,776 in FY 2010. Almost two-thirds of U.S. firms report that they have been the victim of cybersecurity incidents or information breaches. Moreover, this serious problem may be subject to underreporting: only 50 percent of owners and operators at high-priority facilities participating in the ECIP security survey said that they report cyber incidents to external parties. DHS's Strategic National Risk Assessment notes that cyber attacks can have catastrophic consequences and trigger cascading effects across critical infrastructure sectors.[29]

In congressional testimony, the Federal Bureau of Investigation has noted the risks to our critical infrastructure from cyber attacks:

> U.S. critical infrastructure faces a growing cyber threat due to advancements in the availability and sophistication of malicious

27. *See, e.g.*, *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the Subcomm. on Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 16–17, 20–21 (2011) [hereinafter *House Hearings: Data Retention As a Tool for Investigating Internet Crimes*] (statement of John M. Douglass, Chief Of Police, Overland Park, Kansas; International Association of Chiefs of Police, Alexandria, Virginia), *available at* http://judiciary.house.gov/hearings/printers/112th/112-3_63873.pdf.

28. *See, e.g.*, Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, 59 U.S. ATT'YS BULL., Nov. 2011, at 16, 24, *available at* www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf (noting how historical cell site analysis has led to the "identification and arrests of violent felons, including murder suspects, and the rescue of kidnapping and child abduction victims").

29. U.S. DEP'T OF HOMELAND SEC., NATIONAL PREPAREDNESS REPORT 20 (2012), *available at* https://www.hsdl.org/?view&did=707308.

> software tools, and the fact that new technologies raise new security issues that cannot always be addressed prior to adoption. The increasing automation of our critical infrastructures provides more cyber access points for adversaries to exploit.[30]

The impact of cybercrime on national security remains heightened. Earlier this year, Federal Bureau of Investigation Director Robert S. Mueller, III, described multiple avenues in which cybercrime may threaten national security:

> Terrorist use of the Internet is not our only national security concern. As we know, state-sponsored computer hacking and economic espionage pose significant challenges. Just as traditional crime has migrated online, so, too, has espionage. Hostile foreign nations seek our intellectual property and our trade secrets for military and competitive advantage. State-sponsored hackers are patient and calculating. They have the time, the money, and the resources to burrow in, and to wait. They may come and go, conducting reconnaissance and exfiltrating bits of seemingly innocuous information—information that in the aggregate may be of high value. You may discover one breach, only to find that the real damage has been done at a much higher level.[31]

General Keith Alexander, Director, National Security Agency, Chief, Central Security Service and Commander, United States Cyber Command, concluded that cybercrime has resulted in "the greatest transfer of wealth in history."[32] In October, Secretary of Defense Leon E. Panetta described the impact that a targeted cyber attack could have:

---

30. *Cyber Security: Responding to the Threat of Cyber Crime and Terrorism, Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 112th Cong. 122 (2011) (statement of Gordon M. Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112shrg71412/pdf/CHRG-112shrg71412.pdf; *id.* at 6 ("The recent security breach by unauthorized intruders into the parent company of NASDAQ is an example of the kind of breaches directed against important financial infrastructure.").

31. Robert S. Mueller, III, Dir., Fed. Bureau of Investigation, Remarks at RSA Cyber Security Conference (March 1, 2012), *available at* http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies. Other countries have highlighted the threat of cybercrime to national security. *See, e.g.*, PRIME MINISTER'S OFFICE, A STRONG BRITAIN IN AN AGE OF UNCERTAINTY: THE NATIONAL SECURITY STRATEGY, 2010, Cm. 7953, at 1, 29 (U.K.), *available at* http://www.direct.gov.uk/prod_consum_dg/groups/ dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy ("[C]yber security has been assessed as one of the highest priority national security risks to the UK.").

32. Emil Protalinski, *NSA: Cybercrime is 'the Greatest Transfer of Wealth in History'*, ZDNET (July 10, 2012), http://www.zdnet.com/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history-7000000598/; *see also* Emil Protalinski, *Richard Clarke: China Has Hacked Every Major US Company*, ZDNET (Mar. 27, 2012), http://www.zdnet.com/blog/security/richard-clarke-china-has-hacked-every-major-us-company/11125 (quoting former White House cybersecurity and cyberterrorism advisor in stating that "'[e]very major company in the United States has already been penetrated by China. My greatest fear is that, rather than having a

> An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches. They could, for example, derail passenger trains or even more dangerous, derail trains loaded with lethal chemicals. They could contaminate the water supply in major cities or shutdown the power grid across large parts of the country. The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks. The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability.[33]

To counter these growing cyber attacks, law enforcement will need the capacity to trace the manner in which they are committed and to obtain the necessary electronic records. Law enforcement requires sufficient tools to respond to sophisticated cyber attacks in order to uncover and prosecute them.

4. Electronic Records: Many Forms

Criminal Internet activity can result in the creation of many different types of records. Illustratively, such records may include: transactional records which show what Internet Protocol address was used for access and the path of the Internet transmission; text messages or email communications; social networking channels; the uploading or downloading of files or information; steps taken to store information in other places such as in the cloud;[34] the use of peer-to-peer pro-

---

cyber-Pearl Harbor event, we will instead have this death of a thousand cuts. Where we lose our competitiveness by having all of our research and development stolen by the Chinese. And we never really see the single event that makes us do something about it'"); Josh Rogin, *NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History,"* THE CABLE (July 9, 2012), http://thecable.foreignpolicy.com/ posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.

33. Leon E. Panetta, Sec'y, U.S. Dep't of Defense, Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), *available at* http://www.defense.gov/ transcripts/transcript.aspx?transcriptid=5136.

34. "Cloud computing" is defined as:

> [A] model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, THE NIST DEFINITION OF CLOUD COMPUTING: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 2 (2011), *available at* http:// csrc.nist.gov/publi-

grams to share or transfer files; financial transactions online; voice over Internet Protocol communications; the use of someone else's wireless Internet;[35] and log records which show the date and time of activity on the Internet.[36]

The trail of electronic records from the Internet may show: how the crime was committed; reveal communications about planning and preparation; identify who committed the crime or reveal other co-conspirators; identify additional victims; show how money was transferred; corroborate other known evidence; fill in gaps in the evidence; confirm that records were destroyed once the investigation became known; and provide new leads. Electronic evidence might even exclude initial suspects or show that someone was framed. As important as these records may be, they may not be available at the time law enforcement learns about their existence. Based on a provider's retention policy, it may be too late to obtain legal process for these records. This means that key evidence may not be available to help solve a crime.

5. Measuring Loss and the Impact on Society

When crimes are committed using the Internet, the loss to individuals and society can take many forms. There are direct and indirect costs. In some cases, damages have jumped to millions or billions of dollars by impacting numerous individuals and networks.[37]

---

cations/nistpubs/800-145/SP800-145.pdf; *see also* GLOSSARY OF SECURITY TERMS, *supra* note 4, at 35.

35. *See, e.g.*, *infra* note 83 (highlighting the case of *United States v. Ardolf*, in which the defendant used his neighbor's wireless Internet to engage in criminal activity so the defendant's Internet conduct would "be traced back to the neighbor").

36. Mark L. Krotoski & Jason Passwaters, *Using Log Record Analysis to Show Internet and Computer Activity in Criminal Cases*, 59 U.S. ATT'YS BULL., Nov. 2011, at 1, 5 (2011) [hereinafter *Using Log Record Analysis*], *available at* www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf ("In past cases, many providers have maintained log records for only a few days. Other providers may retain the records for a week or so. Some providers may not log all events.").

37. *See, e.g.*, Press Release, Fed. Bureau of Investigation, International Cooperation Disrupts Multi-Country Cyber Theft Ring (Oct. 1, 2010) *available at* http://www.fbi.gov/news/pressrel/ press-releases/international-cooperation-disrupts-multi-country-cyber-theft-ring ("[In Operation Trident Breach, the] cyber thieves targeted small- to medium-sized companies, municipalities, churches, and individuals, infecting their computers using a version of the Zeus Botnet. The malware captured passwords, account numbers, and other data used to log into online banking accounts. This scheme resulted in the attempted theft of $220 million, with actual losses of $70 million from victims' bank accounts."); Press Release, U.S. Dep't of Justice, U.S. Indicts Ohio Man And Two Foreign Residents In Alleged Ukraine-Based "Scareware" Fraud Scheme That Caused $100 Million In Losses To Internet Victims Worldwide (May 27, 2010), *available at* http://www.justice.gov/criminal/

While the true costs of cybercrime are very difficult to gauge,[38] on one level, the loss may be the damages or direct financial impact resulting from the crime. In the criminal justice process, the court will seek to determine restitution to make the victim whole.[39]

The loss will vary depending on the facts of the particular case. In computer hacking cases, for example, loss generally falls into four categories: "[1] the cost of responding to an offense, [2] conducting a damage assessment, and [3] restoring the data, program, system, or information to its condition prior to the offense, and [4] any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[40] In a data breach case, some of the costs may include "detection, escalation, notification and response along with legal, investigative and administrative expenses, customer defections, opportunity loss, reputation management, and costs associated with customer support such as information hotlines and credit monitoring subscriptions."[41]

There are also indirect costs resulting from Internet crime. Businesses may face brand damage and lost customers.[42] Depending on the nature of the crime, individuals may confront mental health and related issues. For example, the trauma resulting from child exploitation can leave scars that remain for many years. The direct costs from child exploitation may include hospitalization, mental health child

cybercrime/press-releases/2010/sundinIndict.pdf; Robert S. Mueller, III, Dir., Fed. Bureau of Investigation, Remarks at Detroit Economic Club (Oct. 16, 2003), *available at* http://www.fbi.gov/news/speeches/protecting-the-u.s.-economy-in-a-global-age (noting that "[b]y the time the 'Love [Bug]' virus had run its course, millions of systems had been disrupted [and the] total damages worldwide were estimated at $8 to $10 billion").

38. The true costs of cybercrime have been difficult to measure because some cybercrime is never reported. Some studies are based on unverified, self-reported information. For example, the recent 2012 Norton Cybercrime Report, which is a survey of 13,000 adults in 24 countries based on self-reported cybercrime, estimated $110 billion annual losses. *See* Press Release, Symantec Corp., Consumer Cybercrime Estimated at $110 Billion Annually (Sept. 5, 2012), *available at* http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02; SYMANTEC CORP., 2012 NORTON CYBERCRIME REPORT 3 (2012), *available at* http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.

39. For more on restitution see *infra* note 68.

40. 18 U.S.C. § 1030(e)(11) (2011) (defining "loss" for offenses under the Computer Fraud and Abuse Act).

41. *Ponemon Study Shows the Cost of a Data Breach Continues to Increase*, PONEMON INST. (Jan. 25, 2010), http://www.ponemon.org/news-2/23.

42. Yuval Ben-Itzhak, *Businesses Under Cybercrime Attack: How to Protect Your Corporate Network and Data Against Its Impact*, CXO (Oct. 8, 2012), http://www.cxo.eu.com/article/Businesses-under-Cybercrime-attack/ ("Once a business or organization is exposed in the media for breaching data, it faces a high chance of brand damage – especially when the media coverage of the breach includes financial and legal details.").

welfare services, and law enforcement responses. The indirect costs may involve special education, juvenile delinquency, mental health care, and the criminal justice system.[43]

As these examples show, the nature of the loss, including direct and indirect costs, will vary depending on the type of case and the facts. The costs of Internet crime have significant consequences for individuals, businesses, and society. The role of law enforcement is to enforce the law, identify the perpetrator(s), hold them accountable in the criminal justice system, and, where possible, seek restitution for the victims.

6. Summary: Without Access to Internet Evidence Through Appropriate Legal Process, the Adverse Impacts from Crimes Committed on the Internet Will Remain Unaddressed

Law enforcement requires the necessary tools to combat cybercrime effectively. For crimes committed on the Internet, the trail of evidence will include records created by the defendant on the Internet. Ensuring that essential electronic data is retained pending appropriate legal process is critical to solving these crimes and redressing the adverse impacts of these crimes on society.

These concerns are not limited to law enforcement. Policy makers and others concerned about cyber attacks on our critical infrastructure, financial institutions and businesses should be concerned about data retention. Parents and families concerned about the exploitation of children should be interested in ensuring that perpetrators can be identified and held accountable. Supporters of the enforcement of other laws enacted by Congress that are violated by using the Internet should care about data retention.

In order to solve crimes committed over the Internet, some of the best evidence necessarily involves Internet records. Obtaining these records in a law enforcement investigation can be challenging; their

43. *See* TED R. MILLER, MARK A. COHEN & BRIAN WIERSEMA, NATIONAL INSTITUTE OF JUSTICE RESEARCH REPORT: VICTIM COSTS AND CONSEQUENCES: A NEW LOOK 1, 12 (1996), *available at* https://www.ncjrs.gov/pdffiles/victcost.pdf (noting "the cost of mental health care for the typical child sexual abuse victim" is much higher than for other crimes); *see generally* CHING-TUNG WANG & JOHN HOLTON, PREVENT CHILD ABUSE AM., TOTAL ESTIMATED COST OF CHILD ABUSE AND NEGLECT IN THE UNITED STATES 2 (2007), *available at* http://www.preventchildabuse.org/about_us/media_releases/pcaa_pew_economic_impact_study_final.pdf (while noting the challenges in estimating the direct and indirect costs of child abuse and neglect, the report provides a conservative estimate of "$103.8 billion in 2007 value" of indirect costs).

availability often turns on whether they are still retained by the provider. Time is usually dispositive. Law enforcement is typically engaged in a race to obtain the electronic evidence as leads are developed while the data is still available from a provider.[44]

B. Following the Trail of Internet Evidence: Obtaining Electronic Evidence Under ECPA

Law enforcement usually obtains these Internet records by meeting the requirements set forth in ECPA.[45] The Stored Communications Act ("SCA"),[46] which is Title II of ECPA, generally regulates access to "stored wire and electronic communications and transactional records"[47] maintained by providers.

By enacting ECPA, Congress weighed different public interests. The House report noted that the ECPA measure "represents a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement."[48] More than a quarter century after ECPA was enacted these competing interests and the question of their proper balance remain; in fact, they are more important today. Related public policy and criminal justice interests, reviewed below in Part I, include: (1) promoting confidence in the use of the Internet; (2) addressing the legitimate needs of law enforcement to investigate

44. This article generally refers to "providers" who furnish Internet services that are subject to the requirements ECPA. ECPA actually distinguishes between "a provider of remote computing service" and "a provider of electronic communications services." *See* 18 U.S.C. § 2510(15) (defining "electronic communications services"); *id.* § 2711(2) (defining "remote computing service"); *see generally* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 117–20 (3d. ed. 2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (explaining and providing examples of remote and electronic communications services).

45. Pub. L. No. 99-508, 100 Stat. 1848 (Oct. 21, 1986). ECPA has three titles: Title I includes the Wiretap Act, which prohibits the interception, use, and disclosure of wire, oral, or electronic communications. *See* 18 U.S.C. §§ 2510–22. Title II contains the Stored Communications Act ("SCA"). *See id.* §§ 2701–12. Title III pertains to the use of pen registers and trap and trace devices. *See id.* §§ 3121–27.

46. 18 U.S.C. §§ 2701–12.

47. H.R. REP. NO. 99-647, at 8 (1986) (Title II-Stored Wire And Electronic Communications And Transactional Records Access).

48. H.R. REP. NO. 99-647, at 16, 19 (1986) ("The purpose of the legislation is to amend title 18 of the United States Code to prohibit the interception of certain electronic communications; to provide procedures for interception of electronic communications by federal law enforcement officers; to provide procedures for access to communications records by federal law enforcement officers; to provide procedures for federal law enforcement access to electronically stored communications; and to ease certain procedural requirements for interception of wire communications by federal law enforcement officers.").

and prosecute crimes committed over the Internet; (3) addressing the rights and interests of crime victims; (4) attaining the public policy objectives identified by Congress in enacting a particular criminal statute; (5) providing a fair process, ensuring that the responsible perpetrators are identified and fairly prosecuted; and (6) balancing and respecting privacy interests.

C. Obtaining Electronic Evidence: Contrasting Case Examples Based on the Availability of Internet Records from the Provider

Two case examples demonstrate the importance of obtaining ECPA records to investigate and prosecute crimes committed, at least in part, on the Internet.[49] One was successful, the other tragically was not. The outcome turned on the availability of records from the provider.

1. Successful Preservation of Emails

First, in *United States v. Xiaodong Sheldon Meng*,[50] a timely law enforcement request to preserve email evidence saved a large number of emails just before someone in another country tried to delete them after the investigation became publicly known.[51] Sheldon Meng, a software engineer at a Silicon Valley high-tech company, was investigated for violating two national security statutes: (1) economic espionage for misappropriating a trade secret from his former employer—software used to simulate real world motion for military training and other purposes—with the intent to benefit a foreign government, specifically the People's Republic of China Navy Research Center;[52] and (2) for exporting source code for a visual simulation software program used for training military fighter pilots, which was a defense article on the United States Munitions List in violation of the Arms Control Export Act.[53] During the investigation, agents submitted a preservation request on known email accounts that the defendant used prior to his arrest. The preservation request saved any informa-

49. This article generally refers to Internet records or electronic evidence, which are normally obtained under ECPA.

50. *See* United States v. Meng, No. CR 04-20216 JF (N.D. Cal. June 11, 2008); *see also* Superseding Indictment at ¶ 37, United States v. Meng, CR 04-20216 JF (N.D. Cal. Dec. 13, 2006) (describing email deletions).

51. For more on the preservation request process under 18 U.S.C. § 2703(f), see *infra* Part II.B.

52. 18 U.S.C. § 1831.

53. 22 U.S.C. § 2778 (2011).

tion in the email account pending legal process; there, a search warrant for the contents of the communications and information stored within the email account. Shortly after the defendant's arrest in Florida became publicly known, someone using an Internet Protocol address[54] from the People's Republic of China tried to delete virtually all of the emails from his account while he was in custody.[55] The effort to delete the emails was thwarted by the timely preservation request. The emails were subsequently obtained by a search warrant and used in the investigation and prosecution of the case. Without these email communications, the scope of the defendant's conduct and activities would have been less known. If law enforcement had first learned about these accounts later, such as after his arrest, most likely any effort to preserve the emails would have been in vain given how quickly someone acted to delete information in the account from another country. Fortunately, because these records were preserved, the effort to remove and destroy them was thwarted.

2. Unavailability of Records Results in Case Closure

In contrast, a case noted during congressional testimony shows how a horrific crime remained unsolved when a provider no longer retained account records. The crime involved an atrocious rape of a two-year-old child that was videotaped and distributed on the Internet. Investigators acted quickly in attempting to identify the responsible

54. Every computer connected to the Internet is assigned a unique Internet Protocol ("IP") address by an Internet Service Provider. IP addresses consist of four numbers separated by periods, such as: 12.34.567.789.

55. Government's Sentencing Memorandum at 8, United States v. Meng, No. CR 04-20216 JF (N.D. Cal. June 11, 2008). Investigators learned that someone deleted more than 900 e-mails from the defendant Meng's Yahoo e-mail account. *Id.* In early December 2004, defendant Meng's e-mail account contained approximately 980 emails. *Id.* Between December 9, 2004 and January 2, 2005, defendant Meng was being held in custody by the United States government and could not access his email account. *Id.* Between December 22, 2005 and January 2, 2005, someone utilizing IP addresses in China, accessed Meng's Yahoo email account and deleted approximately 966 emails. *See* Superseding Indictment at ¶ 37, United States v. Meng, CR 04-20216 JF (N.D. Cal. Dec. 13, 2006) (describing email deletions); *Electronic Evidence In EEA Cases*, *supra* note 18, at 47–48 (summarizing preservation of emails). The authors prosecuted the *Meng* case during their tenure in the U.S. Attorney's Office in the Northern District of California. Meng ultimately pled guilty to committing economic espionage and violating the Arms Export Control Act. *See* Plea Agreement, United States v. Meng, No. CR 04-20216 JF (N.D. Cal. Aug. 29, 2007) (as redacted by the Court); Press Release, Dep't of Justice, Former Chinese National Convicted of Economic Espionage to Benefit China Navy Research Center (Aug. 2, 2007), *available at* http://www.justice.gov/opa/pr/2007/August/07_nsd_572.html; Press Release, Dep't of Justice, Chinese National Sentenced for Economic Espionage (June 18, 2008), http://www.justice.gov/ opa/pr/2008/June/08-nsd-545.html.

party. In pursuing the offense, an investigator determined that a video of the incident was linked to a particular computer. An Internet Service Provider ("ISP") was contacted for the account information for the computer. Regrettably, investigators were informed that the provider had not retained the customer records. There was nothing more investigators could do and the crime remained unsolved without this critical information.[56] Unfortunately, this is not an isolated case. Other comparable investigations have been closed once necessary Internet records were unavailable for the ongoing investigation.[57]

Both of these examples involved criminal activity over the Internet. In both instances, key evidence was initially maintained by providers. In the first case, law enforcement was able to obtain information retained in the account by a timely preservation request.[58] Key details concerning the charges were provided by email evidence that would not have otherwise been available. In the second case, law enforcement acted as quickly as it could after receiving the Internet in-

56. *Sexual Exploitation of Children Over the Internet: What Parents, Kids and Congress Need to Know About Child Predators: Hearings Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 109th Cong. 285, 287 (2006) (statement of Mr. Flint Waters, Lead Special Agent of the Wyoming Division of Criminal Investigations, Internet Crimes Against Children Task Force), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-109hhrg30793/pdf/CHRG-109hhrg30793 .pdf; *see also* STAFF REPORT: SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET, *supra* note 20, at 19 ("When the ICAC agent approached the Internet Service Provider, Comcast, to request the customer information for the IP address in Colorado, Comcast informed the agent that it had not retained the customer records for that address. As of the date of the hearing, to Mr. Waters' knowledge, the child in the video had not been identified.").

57. Similar problems have occurred in other child sexual exploitation cases. *See Protecting Children From Internet Pornographers Act of 2011: Hearing on H.R. 1981 Before the Subcomm. on Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 35– 36, 60 (2011) [hereinafter *House Hearing: Protecting Children*] (statement of Michael J. Brown, Sheriff, Bedford County Sheriff's Office, Retired), *available at* http://judiciary.house.gov/hearings/printers/112th/112-60_67309.pdf (law enforcement received a cyber-tip from the National Center for Missing and Exploited Children in February 2011 involving "someone posting that they were exposing themselves to their 2-and-a-half-year-old child"; the "only piece event evidence" was the Internet Protocol address in a chat room; because the Internet Service Provider only retained the Internet Protocol history for 30 days, which had already passed, the case was closed; comparable case closures have occurred "on a number of occasions"); *Sexual Exploitation of Children Over the Internet: How the State of New Jersey Is Combating Child Predators On The Internet: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. of Energy and Commerce*, 109th Cong. 34, 62 (2006) [hereinafter *House Hearing: New Jersey Is Combating Child Predators On The Internet*], *available at* http://www.gpo.gov/fdsys/pkg/CHRG-109hhrg30531/pdf/CHRG-109hhrg30531.pdf (noting that out of 110 investigative leads for possession and distribution of child pornography over the Internet in Operation Guardian, only 39 targets were arrested because information was not retained by Internet Service Providers for the other leads).

58. As discussed in Part II.B, there are significant limitations to the preservation of Internet records.

vestigative lead. However, law enforcement ran into an investigative dead end because the provider did not retain the requested identity information. Since this information was no longer available, law enforcement was unable to identify the involved parties and the case was closed.

3. Summary

The ability of law enforcement to obtain electronic records turned on their availability from the provider. In both instances, law enforcement acted promptly based on known information. The sole difference was that in the first instance, the provider still had the records. In the second, the provider did not. These examples illustrate the race that law enforcement engages in when pursuing new leads based on Internet records. Whether the records are available or not will be unknown until legal process is served on the provider.

I. Significant Public Interests Impacted by the Availability of Internet Records

Key public interests are affected by the availability of electronic records to solve crime. Six key public policy objectives include: (1) promoting confidence in the Internet; (2) addressing the legitimate needs of law enforcement to investigate and prosecute crimes committed over the Internet; (3) addressing the rights and interests of crime victims; (4) attaining the specific public policy objectives identified by Congress in enacting a particular criminal statute; (5) provide a fair process, ensuring that the responsible perpetrators are identified and fairly prosecuted; and (6) balancing and respecting privacy interests.

A. Promoting Confidence in Using the Internet

The Internet is now an integral part of our social and economic fabric. Many persons are nearly always connected to the Internet either at work, home or in between through portable devices. E-commerce transactions are used to purchase nearly any item online. Next year, e-commerce sales in the United States alone are expected to pass $250 billion.[59]

59. D. Steven White & Godwin C. Ariguzo, *A Time-Series Analysis of U.S. E-Commerce Sales*, 11 Rev. Bus. Research 134, 139 (2011) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1940960 ("By 2013, it is predicted that U.S. e-commerce sales will reach a level of $254.7 billion, for a growth in e-commerce sales of 52.94 percent from 2010.").

The Internet makes a significant contribution to the economy domestically and around the world.[60] The Internet has spawned new economic opportunities.[61] For example, the Internet promotes new economic activity through lower transaction costs.[62] Application developers find new ways and develop new tools to use on the Internet. Mobile devices are now being used to conduct an increasing number of online transactions.[63] Small businesses use the Internet as a gateway to reach customers with whom they may not otherwise be able to connect. Indeed, for many, it is now difficult to imagine one day or a few hours without connecting to the Internet in one form or another.

When Internet crimes remain unsolved or unaddressed, a loss of confidence may result in the use of the Internet for e-commerce and other Internet transactions and activities. For example, one international report noted the impact of malware crimes on the confidence of users of the Internet:

> Society's heavy reliance on information systems makes the consequences of the failure or compromise of those systems potentially serious. Malware is an effective and efficient means for attackers to compromise large numbers of information systems, which cumulatively has the potential to undermine and erode society's ability to trust the integrity and confidentiality of information traversing these systems. The failure to provide adequate protection for the confidentiality and integrity of online transactions may have implications for governments, businesses and consumers. For example, electronic government (e-government) services, such as online fil-

60. *See, e.g.*, U.S. CENSUS BUREAU, E-STATS 3 (2012) *available at* http://www.census.gov/ econ/estats/2010/2010reportfinal.pdf ("From 2002 to 2010, retail e-sales increased at an average annual growth rate of 17.9 percent, compared with 2.6 percent for total retail sales."); MCKINSEY GLOBAL INSTIT., INTERNET MATTERS: THE NET'S SWEEPING IMPACT ON GROWTH, JOBS AND PROSPERITY (2011), *available at* http://www.mckinsey.com/features/~/media/ 6BDDD3D756C449C1A9C41633EE5B0732.ashx (noting that "the Internet has been a major driver to economic growth and is getting stronger").

61. *See, e.g.*, United Nations Conference on Trade and Development (UNCTAD), *Building Confidence: Electronic Commerce and Development,* at 18, U.N. Doc. UNCTAD/SDTE/Misc. 11 (2000) [hereinafter *Building Confidence*], *available at* http://unctad.org/en/Docs/posdtem11.en.pdf (noting "the speed, range and accessibility of information on the Internet and the low cost of distributing and capturing it create new commercial possibilities").

62. *See, e.g.*, *Building Confidence*, *supra* note 61 ("[T]he Internet reduces transaction costs and thus stimulates economic activity. A banking transaction via the Internet costs one cent, compared with 27 cents at an ATM or 52 cents over the telephone. Processing an airline ticket on the Internet costs $1, compared with $8 through a travel agent . . . .").

63. *See, e.g.*, Peter Eckert, *Impact of Mobile Devices on Ecommerce,* MOBILE COMMERCE DAILY (July 17, 2012), http://www.mobilecommercedaily.com/impact-of-mobile-devices-on-ecommerce (predicting "that globally $119 billion in goods and services will be purchased via a mobile phone in 2015, representing about 8 percent of the total ecommerce market").

> ing for taxes or benefits, are likely to include personal data that if compromised could be used to commit fraud. Information systems in small businesses or large public and private sector organisations might be used to access such e-government or electronic commerce (e-commerce) services.[64]

A joint law enforcement report echoed this point concerning an "erosion" of public confidence with regard to "phishing" schemes:

> Phishing also undermines the public's trust in the Internet. By making consumers uncertain about the integrity of commercial and financial websites, and even the Internet's addressing system, phishing can make them less likely to use the Internet for business transactions. People who cannot trust where they are on the World Wide Web are less likely to use it for legitimate commerce and communications.[65]

Given the importance of the Internet globally and domestically, the ability of law enforcement to obtain Internet records upon sufficient legal process remains integral to the public policy interest in maintaining confidence in the Internet.

B. "Legitimate Needs Of Law Enforcement"

Law enforcement is tasked with investigating and prosecuting crimes. This objective cannot be met unless law enforcement has reasonable means to investigate crimes committed over the Internet. An important criminal justice objective is to ensure that law enforcement has appropriate mechanisms to obtain key evidence and information when it is needed. If essential Internet records are not available upon a proper showing, then law enforcement simply may not be able to complete its primary objectives. It is like asking law enforcement to be successful without the means to do so.

In fact, by enacting ECPA, Congress initially recognized that the "legitimate needs of law enforcement" is an essential public policy interest.[66] Not only does this objective continue, it is even more important today. The Internet is used more frequently to commit crimes today than when ECPA was enacted in 1986 and there are more ways in which Internet crimes can be committed.

Given the limited retention of Internet records, normally law enforcement is racing to obtain this evidence as investigative leads are provided. The process of identifying, preserving, requesting, and ob-

64. MALWARE REPORT, *supra* note 4, at 41.

65. REPORT ON PHISHING, *supra* note 1, at 11 (footnote omitted). For a definition of "phishing," *see supra* note 13.

66. *See* H.R. REP. NO. 99-647, at 19 (1986).

taining Internet evidence entails many steps.[67] Delays in the process hamper the ability of law enforcement to enforce the law. Since time is of the essence, even one day can make all the difference to whether the necessary evidence to solve the crime may be obtained.

C. Crime Victims' Rights and Interests

Another public policy interest identified by Congress is serving the needs of crime victims in the criminal justice process. Crime victims turn to law enforcement to investigate the offense, seek justice through the criminal justice process, and to obtain restitution or be made whole to the extent possible.[68] Significant victims' rights statutes provide important protections once the criminal justice process has commenced.[69]

Generally, since enactment of the Crime Victims' Rights Act, crime victims are "full participants in the criminal justice system."[70] Crime victims have eight specific statutory rights:

> (1) The right to be reasonably protected from the accused;
> (2) The right to reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime or of any release or escape of the accused;
> (3) The right not to be excluded from any such public court proceeding, unless the court, after receiving clear and convincing evidence, determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding;

67. The steps are described *infra* Part II.C.

68. Restitution is mandatory in many criminal cases. *See* 18 U.S.C. § 3556 (2006) (order of restitution); *see generally id.* § 3663A (mandatory restitution to victims of certain crimes); *id.* § 3663 (order of restitution); *id.* § 3664 (procedure for issuance and enforcement of order of restitution); *id.* § 3771(a) (noting restitution right). Restitution may also be ordered as a condition of probation or supervised release. *See id.* § 3563(b)(2) (probation condition); *id.* § 3583(d) (supervised release condition).

69. *See generally* Victims' Rights and Restitution Act, 42 U.S.C. § 10607 (2006) (services for victims); Crime Victims' Rights Act ("CVRA"), 18 U.S.C. § 3771; 18 U.S.C. § 3510 (rights of victims to attend and observe trial). The Department of Justice has implemented Procedures to Promote Compliance with Crime Victims' Rights Obligations as well. *See* 28 C.F.R. § 45.10 (2011).

70. Kenna v. United States District Court, 435 F.3d 1011, 1016 (9th Cir. 2006) (granting a petition for writ of mandamus and holding that the district court erred by refusing to permit crime victims to speak at a sentencing hearing, while noting that "[l]imiting victims to written impact statements, while allowing the prosecutor and the defendant the opportunity to address the court, would treat victims as secondary participants in the sentencing process. The CVRA clearly meant to make victims full participants"); *see also In re* Stewart, 552 F.3d 1285, 1289 (11th Cir. 2008) (per curiam) (after district court denied victims' request to be heard before a plea hearing, granting petition for a writ of mandamus and ordering the district court "to recognize petitioners as victims and afford them the rights of victims under the CVRA").

> (4) The right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding;
>
> (5) The reasonable right to confer with the attorney for the Government in the case;
>
> (6) The right to full and timely restitution as provided in law;
>
> (7) The right to proceedings free from unreasonable delay; and
>
> (8) The right to be treated with fairness and respect while preserving the dignity and privacy of the victim.[71]

However, for Internet-based offenses, if key electronic evidence is not available, the crime may be unsolvable and no charges may be filed. In such instances, crime victims may never have an opportunity to seek redress in the criminal justice process.[72] None of the foregoing rights will apply. There will only be a victim without justice and the right to be "reasonably heard" in the criminal justice process.

Electronic evidence may also be necessary to identify other crime victims. This evidence may reveal that the scope and impact of the offense is broader than originally anticipated when the investigation commenced. It is not uncommon that as the investigation begins only one or a few victims are known. As the investigation progresses, investigators may learn that multiple people may have been victimized by the same scheme or offense. An accurate accounting of victims may be necessary to properly determine restitution and attain the congressional objective promoting restitution.

The ability of law enforcement to obtain necessary Internet records is therefore central to advancing and attaining the policy objectives recognized by Congress to vindicate the rights of victims. Without crucial evidence available only from providers, Internet crime victims may never see the criminal justice process remedy their wrongs.

---

71. 18 U.S.C. § 3771(a).

72. Courts have noted that the Crime Victims' Rights Act "does not confer any rights upon a victim until a prosecution is already begun." United States v. Merkosky, No. 1:02CR-0168-01, 2008 WL 1744762, at *2 (N.D. Ohio Apr. 11, 2008); *see also* United States v. Rubin, 558 F. Supp. 2d 411, 429 (E.D.N.Y. 2008) (noting that the rights of crime victims did not commence until charges were filed which triggered "covered status under the CVRA"); The Availability of Crime Victims' Rights Under the Crime Victims' Rights Act of 2004, 35 Op. O.L.C. 1, 4 (2010), *available at* http://www.justice.gov/olc/2010/availability-crime-victims-rights.pdf ("In our view, the better reading of the Act—considering its text, structure, purpose, and legislative history—is that the rights provided by the CVRA are guaranteed only from the time criminal proceedings are initiated through a complaint, information, or indictment.").

D. Public Policy Objectives for Specific Criminal Statutes

Many statutes are enacted by Congress to advance specific and unique objectives. In doing so, Congress has already determined that certain public policy interests are important. For every statute, Congress makes a public policy decision concerning the societal importance of redressing certain crimes by the fact that the statutes are enacted. The legislative objectives for the specific offenses may be frustrated without important electronic evidence. A few examples are considered.

1. Economic Espionage Act of 1996

The Economic Espionage Act ("EEA") of 1996 was enacted to promote and protect national economic security.[73] As noted in the House Report:

> With this legislation, Congress will extend vital federal protection to another form of proprietary economic information — trade secrets. There can be no question that the development of proprietary economic information is an integral part of America's economic well-being. Moreover, the nation's economic interests are a part of its national security interests. Thus, threats to the nation's economic interest are threats to the nation's vital security interests.[74]

In signing the legislation into law, President William Clinton noted the statute's necessity to protect trade secrets which "are an integral part of virtually every sector of our economy and are essential to maintaining the health and competitiveness of critical industries operating in the United States."[75] If the trade secret or economic espionage offense was committed in part over the Internet, and these electronic records are not available, the ability to investigate and pros-

73. *See* Pub. L. No. 104-294, 110 Stat. 3488 (codified as amended 18 U.S.C. §§ 1831–1839).

74. H.R. REP. NO. 104-788, at 4 (1996); *see also Economic Espionage: Hearing Before the House Judiciary Subcommittee on Crime of the H. Comm. on the Judiciary*, 104th Cong. 13–14 (1996) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) (noting the inability of existing law to counter state-sponsored targeting of "persons, firms, and industries in the United States and the U.S. Government itself, to steal or wrongfully obtain critical technologies, data, and information in order to provide their own industrial sectors with a competitive advantage" and that "[c]losing these gaps requires a federal statute to specifically proscribe the various acts defined under economic espionage and to address the national security aspects of this crime").

75. Presidential Statement on Signing the Economic Espionage Act of 1996, 3 PUB. PAPERS 2040 (Oct. 11, 1996); *see also* H.R. REP. NO. 104-788, at 4 (noting that "the development of proprietary economic information is an integral part of America's economic well-being" and "threats to the nation's economic interest are threats to the nation's vital security interests").

ecute the offense may be thwarted. Many of these cases have been shown to involve email and Internet communications.[76] The congressional objective to promote and protect national economic security is undermined absent effective law enforcement means to secure critical online information.

2. Identity Theft Penalty Enhancement Act of 2004

As another example, Congress sought to curb "the growing problem of identity theft" by providing for enhanced penalties in the Identity Theft Penalty Enhancement Act of 2004.[77] This policy objective is undermined by the inability of law enforcement to obtain electronic evidence particularly since the Internet is a common forum to commit identity theft. Higher penalties cannot be levied if the perpetrators are not identified and held accountable in the criminal justice process in the first instance.

3. Protection of Children Against Sexual Exploitation Act of 1977

In a third example, Congress enacted the Protection of Children Against Sexual Exploitation Act of 1977,[78] to address "a deep and abiding concern for the health and welfare of the children and youth of the United States" and "to protect and benefit such children."[79] The Senate Report described the exploitation as a unique "form of child abuse" which "may permanently traumatize and warp the minds of the children involved."[80] The children are often impacted for many years. "Such encounters cannot help but have a deep psychological, humiliating impact on these youngsters and jeopardize the possibility of healthy, affectionate relationships in the future."[81]

We do not need to hypothesize about what might happen when law enforcement is unable to obtain Internet records related to the

76. *See Electronic Evidence In EEA Cases*, *supra* note 18, at 43–46 (providing examples of electronic evidence used in trade secret and economic espionage cases).

77. *Identity Theft Penalty Enhancement Act, and the Identity Theft Investigation and Prosecution Act of 2003: Hearing on H.R. 1731 and H.R. 3693 Before the Subcomm. on Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary*, 108th Cong. 1 (2004), *available at* http:// judiciary.house.gov/legacy/92671.pdf; *see also* Pub. L. No. 108-275, 118 Stat. 831 (codified at 18 U.S.C. §§ 1028, 1028A).

78. Pub. L. No. 95-225, 92 Stat. 7 (codified at 18 U.S.C. § 2252 (1982)).

79. *Protection of Children Against Sexual Exploitation: Hearings Before the Subcomm. to Investigate Juvenile Delinquency of the S. Comm. on the Judiciary*, 95th Cong. 6 (1977), *available at* http:// ia600309.us.archive.org/24/items/protectionofchil00unit/protectionofchil00unit.pdf.

80. *Id.* at 41, 47, 48, 52.

81. *Id.* at 46.

sexual exploitation of children on the Internet. Tragically, we already have several concrete examples of how open investigations must be closed when this electronic evidence is not available.[82] During congressional hearings, Congress has been told on at least three occasions that if the necessary Internet records had been retained, further investigation could have been pursued. Perhaps these open cases may have been solved. Because necessary Internet records were unavailable, all that is left is a scarred and traumatized child without redress in the criminal justice process. When this occurs, the objectives of Congress in enacting the original Protection of Children Against Sexual Exploitation Act, as amended over the years, are thwarted by the unavailability of key Internet evidence.

4. Summary

These are only a few illustrations of the objectives noted in criminal statutes. Each congressional statute has a unique public policy purpose that it seeks to address. When the crime remains unsolved as a result of the unavailability of Internet records, these congressionally identified objectives are frustrated.

E. Due Process Interests: Identifying the Right Perpetrator and Providing a Fair Trial

The criminal justice process also advances important due process interests for the accused. This includes the objectives to identify the correct perpetrator(s) and to provide a fair trial.

Electronic evidence can be used to support guilt or innocence. For example, in some cases the defendant has used the accounts of others or tried to set up another individual to make it appear that he was involved.[83] The initial leads in these cases suggest that the person

82. For specific examples, see *supra* notes 55–56.

83. *See, e.g.*, United States v. Middleton, 231 F. 3d 1207, 1208 (9th Cir. 2000) (affirming hacking trial conviction and describing how the disgruntled computer administrator defendant accessed the company's network after he quit his position and "used a computer program called 'Switch User' to switch his account to that of a [company receptionist which allowed him] to take advantage of the benefits and privileges associated with that employee's account, such as creating and deleting accounts and adding features to existing accounts"); United States v. Ardolf, No. 10-159, 2010 WL 3604099 (D. Minn. Aug. 13, 2010). In *Ardolf*, the defendant tried to set up his neighbor by using his neighbor's wireless Internet account. *See* Press Release, U.S. Dep't of Justice, U.S. Att'ys Office, Dist. Minn., Blaine Man Sentenced for Hacking into Neighbor's Internet System to Email Threats Against the Vice President, Among Other Crimes (July 12, 2011). The defendant admitted hacking into the account, creating email accounts in his neighbor's name, and using one account to send threatening communications to the Vice President of the

being set up was involved in the crime under investigation. The Internet records, if available, can be used to determine how the offense was committed and who was behind it. In this way, the Internet records promote the criminal justice objectives of ensuring that the right perpetrator is identified and held to account. Without necessary records, a full understanding of how the crime was committed over the Internet may remain unknown. The trail of Internet evidence often provides an explanation or understanding for other gaps in the evidence. In this manner, the ultimate criminal justice interest in ensuring a fair trial is promoted.

F. Balancing and Respecting Privacy Interests

As originally enacted, ECPA recognized the public policy interest in "the privacy expectations of citizens."[84] These privacy interests remain important today but should be appropriately balanced against other significant public policy interests, specifically law enforcement and victims' rights interests.

Privacy concerns can be balanced in a number of respects. First, the legal process considers privacy concerns when law enforcement seeks to obtain the requested information. No records are provided unless proper legal process is submitted. Legislative and other proposals to retain electronic records recommend that pre-existing records be retained for a longer period.[85] Providers are not compelled to create new records,[86] they have already determined that these records serve their business purposes. These pre-existing records are not relin-

United States and other officials. *Id.* The defendant "admittedly sent the email using the neighbor's wireless router, his intent being to have the email traced back to the neighbor." *Id.* He also "posed as his neighbor and used the email accounts he had created to send emails of a sexual nature to three of the neighbor's co-workers" using "the neighbor's wireless Internet connection, intending for them to be traced back to the neighbor." *Id.* He "attached an image containing child pornography" to one email message, and "created a MySpace page in the neighbor's name, on which he posted the same image of child pornography." *Id.* Defendant was sentenced to 216 months in prison following his plea agreement conviction based on two counts of aggravated identity theft, one count of distribution of child pornography, one count of possession of child pornography, one count of unauthorized access to a protected computer, and one count of making threats to the President and successors to the presidency. *Id.*

84. *See* H.R. REP. NO. 99-647, at 19 (1986).

85. Recent legislative proposals are considered below. *See infra* Part IV.C.

86. *See, e.g.*, *House Hearings: Data Retention As a Tool for Investigating Internet Crimes*, *supra* note 27, at 50 (addressing privacy concerns noting that much of the data is already presently being retained by providers and that "[a] mandatory data retention requirement would only extend that retention time to make sure that it was applied universally across industry" and available for law enforcement).

quished to law enforcement unless sufficient legal process is obtained. The retention of electronic communications is merely preserved pending legal process. The balance of privacy interests against the "legitimate needs of law enforcement" is struck by the inability to obtain any records absent sufficient legal process.[87] As noted, the preservation process under Section 2703(f) works well but has significant limitations.[88] If the records are not present at the time law enforcement learns about them and requests them, the legitimate needs of law enforcement cannot be met.

Second, privacy concerns are considered by the legal standard required to obtain electronic records—depending on the nature of the records. The standard for obtaining records under the current law is higher when the contents of communications are requested. Under ECPA, a search warrant is generally required to obtain the "contents of a wire or electronic communication."[89] Lesser standards are used for transactional and other records that do not involve the contents of communications.[90] As the Supreme Court has recognized, there is no reasonable expectation of privacy in records that are voluntarily given to third parties such as subscriber information or transactional records.[91] In following the trail of evidence on the Internet, law enforcement is largely seeking records that the defendant voluntarily conveyed to third party Internet providers during the commission of the crime.

Third, privacy concerns have been sufficiently addressed with regard to the retention of other records in which mandatory retention standards apply. For example, health, employment, banking and other records must satisfy retention periods ranging from one to ten

87. *See* H.R. REP. NO. 99-647, at 16, 19.

88. For a discussion of the preservation process and limitations, see *infra* Part II.B.

89. 18 U.S.C. § 2703(a) (2006).

90. For a summary of these standards, see *infra* note 99.

91. *See* United States v. Miller, 425 U.S. 435, 440 (1976) (holding there was no "legitimate 'expectation of privacy'" under the Fourth Amendment in bank records which were "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business" and were not his "private papers"); Smith v. Maryland, 442 U.S. 735, 744 (1979) (applying *Miller* and holding that there was no reasonable expectation of privacy in dialed telephone numbers obtained from the phone company). In *Smith* the Court noted that "[w]hen [petitioner] used his phone, [he] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed." *Id.* Since there is no Fourth Amendment right in records voluntarily conveyed to third parties, Congress can weigh the balance of interests and determine the circumstances in which law enforcement can access these records in a manner that does not undermine law enforcement objectives.

years, depending on the records.[92] Many of these records are now maintained in electronic form. The sufficient safekeeping of these types of records, many of which include the most private of information, shows that privacy issues can be respected and satisfied.

Fourth, the privacy interests of a customer of a particular account served by a provider have already been breached when the customer becomes a crime victim.[93] In this situation, the account holder will usually turn to law enforcement for assistance. As already noted, whether the victim will obtain justice, restitution, and other crime victim rights, will turn on the ability of law enforcement to investigate and solve the crime by obtaining records establishing who committed the crime.

Finally, in retaining the data, steps can be taken to ensure that it is sufficiently safeguarded. Because data must be searchable, it cannot be encrypted. Nevertheless, other steps can be taken to safeguard it. For example, many providers do not allow access to these records from within the company unless there is a business reason for the access. Further, law enforcement will not be able to obtain the records absent a sufficient showing.

In sum, concerns about privacy interests remain important. They can be addressed by the manner and circumstances in which law enforcement may request and obtain the records.

II. Key Challenges in Obtaining Fleeting Electronic Evidence

While electronic records may be essential to solving Internet-based crimes and advancing the several public policy interests noted above, law enforcement confronts a host of challenges in obtaining this critical and time sensitive evidence. Insufficient retention polices compound the problem created by electronic evidence's ephemeral nature. Because electronic evidence is typically only available for a very limited period, delays in learning about the account or in obtaining an investigative lead are inherent in the process.

92. For a discussion of some of the retention records, see *infra* notes 94–98 and accompanying text.

93. The commission of the crime on the Internet may cause an invasion of privacy for the crime victim. As Federal Bureau of Investigation Director Mueller has noted on this point, "[w]henever an intruder opens a door to our networks, there is a clear risk to individual privacy and intellectual property—not to mention economic and national security." Robert S. Mueller, III, Dir., Fed. Bureau of Investigation, Address at the Commonwealth Club of California (Oct. 7, 2009), *available at* http://www.fbi.gov/news/speeches/cloak-and-dagger-in-the-virtual-world-the-fbi2019s-fight-against-cyber-threats.

A. Limited Period of Availability Based on Retention Period

In following the trail of Internet evidence, there are many electronic records that are created that may be relevant to investigating the offense. Most Internet records are available for only a limited period. Their availability turns on how long a provider retains the records. There is no uniform period of retention. Different types of records have different retention periods.[94] Each provider determines what and how records are maintained based on their unique business needs.[95]

For example, text message content is typically retained for only a few days. Log records, which record commands and other information transmitted through the Internet and may reveal Internet activity by a user, also are usually maintained for only a few days.[96] Subscriber information and method of payment for the account may be held for a longer period.[97]

There is also a lack of uniformity in how the same or similar records may be maintained by different providers. Records that may be retained by one provider for one week may be retained by a different provider for only a few days. For example, text messages normally are retained, if at all, for a short period, typically a few days or a week. If text communications by customer A using provider A are sent and

94. The different retention periods have also been noted during congressional hearings. *See, e.g.*, *Making The Internet Safe For Kids: The Role Of ISP's And Social Networking Sites: Hearings Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 109th Cong. 12 (2006) [hereinafter *House Hearings: Making the Internet Safe*] (statement of Rep. Michael C. Burgess), *available at* http://www.gpo.gov/fdsys/search/pagedetails.action?st=search+algorithms&granuleId=CHRG-109hhrg30530&packageId=CHRG-109hhrg30530&bread=true ("While some of the providers, like EarthLink, retain data for 7 years, others retain the IPs for as little as 31 days."); *id.* at 96, 144–45, 149, 281 (noting that IP addresses are retained for 180 days by Comcast, seven years by Earthlink, 90 days by AOL, nine months by Verizon, and 90 days by MySpace.com); STAFF REPORT: SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET, *supra* note 20, at 22 (noting during congressional hearings that "the data retention policies of the ISPs that testified at the hearing vary widely, from 60 days to seven years"); *Electronic Evidence In EEA Cases*, *supra* note 18, at 47 (providing examples of retention periods for different types of records).

95. If one provider elects to retain more records than another provider for its own business reasons, upon sufficient legal process law enforcement should be able to access these preexisting records, which may prove essential to solving the crime.

96. For more background on the use of log records in criminal investigations, see *Using Log Record Analysis*, *supra* note 36.

97. The Stored Communications Act provides for disclosure to law enforcement customer or subscriber information including name, address, telephone connection records, or records of session times and durations, length of service, types of service utilized, subscriber identity, and means and source of payment for services rendered. 18 U.S.C. § 2703(c)(2) (2006).

received by customer B using provider B, the ability for law enforcement to obtain these communications may turn on which provider retains them longer. If the crime is reported after the retention period, these records cannot be obtained from either provider.

B. The Preservation of Records, While Useful, Has Significant Limitations

ECPA has an important preservation provision under Section 2703(f),[98] which provides an important tool for law enforcement. Upon a preservation request by law enforcement, a provider will freeze or take a "snapshot" of available electronic records in the account which is held pending legal process (such as a search warrant, court order or subpoena).[99]

For example, if an investigator learns of an Internet account (such as an email account or Internet Protocol address),[100] a preservation request is sent to the email provider and held for 90 days until legal process is obtained and submitted to the provider. The 90 day preservation can be extended once more for an additional 90 days. A search warrant will be prepared and submitted to a judge if the contents of the account are sought.[101] Once the search warrant is signed

98. The preservation provision provides:

> (1) In general. — A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.
>
> (2) Period of retention. — Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

18 U.S.C. § 2703(f).

99. Legal process may include: (1) a search warrant based on probable cause under the Fourth Amendment and issued under 18 U.S.C. § 2703(a) for the content of electronic or wire communications maintained by a provider; (2) a court order under 18 U.S.C. § 2703(d) based on "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation" that provides for subscriber and customer account information and other non-content records concerning an account, such as transactional logs; (3) a subpoena under 18 U.S.C. § 2703(c)(2) to obtain subscriber and customer account information; and (4) a pen register or trap and trace order under 18 U.S.C. §§ 3121–27 for records of outgoing and incoming telephone or electronic communications to a particular number or account.

100. An Internet Protocol address is assigned by an Internet service provider and is used to access the Internet. The IP address is comparable to a telephone number assigned to a particular house or place.

101. A search warrant may be submitted for "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for more than one hundred and eighty days or less . . . ." 18 U.S.C. § 2703(a).

by the judge, it will be submitted to the provider. The provider will comply with the legal process and collect the records within the scope of the search warrant. The information, which can take some time to gather, will then be provided to law enforcement. The information may provide new leads about previously unknown accounts. New preservation requests may be issued on these new leads. A new round to obtain legal process commences on the new leads.

1. Limited to Preservation or "Snapshot" of Information Pending at the Time of the Request

There are two significant limitations to preservation requests. First, preservation is limited to what remains in the account at the time of the preservation request. Even if the account is known or later becomes known, it is helpful if the data is present at the time of the request for preservation but often it is not. There is often a substantial gap between the time that a record is created and retained by a provider and the time that law enforcement may first learn about it and request preservation. A preservation request for an account that is empty or in which key communications have been removed will yield no substantive results for the investigation.

Timing is therefore dispositive. Because of varying retention periods, the availability of Internet-based records largely turns on time. One day can make a difference in obtaining the evidence. However, the longer the retention period, the greater the chance that key electronic records will be available pending law enforcement process.

2. The "Electronic Evidence Lapse" Problem

The second challenge results from the lapse of electronic evidence that invariably become known as the investigation develops. The limited retention of records creates a race to identify all relevant electronic evidence leads. However, by the time that law enforcement learns about subsequent leads, those newly identified electronic records may no longer be available if the retention period has already passed by the time they were discovered.

It is not uncommon that one Internet lead may result in the discovery of other accounts and Internet evidence. If the originally preserved records contain new leads, one question will be whether information in these newly identified accounts will be available by the time law enforcement learns of these leads and legal process is submitted for these new accounts and the information is received. The lapse of these records may make a difference in the investigation.

This is important because new leads are often generated as electronic evidence is obtained pursuant to legal process. An initial preservation and request for Internet records often highlights new Internet records, resulting in a second preservation and request, which may lead to a third preservation and request, and so on. For example, an account may not become known until further electronic evidence is uncovered after pursuing numerous leads over several months. Later in the investigation, information about new accounts may surface. However, due to limited retention periods, the records for the second or third or later request may no longer be available at the time law enforcement first learns about them. The longer the information is retained pending legal process the more likely it may be available for law enforcement purposes upon its discovery.

In law enforcement's race to obtain Internet records, timing may determine whether these records are still retained at the time law enforcement first learns of their relevance to the investigation. This "electronic evidence lapse" may impact whether the crime can be solved.[102]

C. Under ECPA, There Are Many Steps in the Investigative Process to Obtain Electronic Records

The process of identifying, preserving, requesting, and obtaining Internet evidence through the legal process is often not fully appreciated or understood. Given the limited retention periods for many Internet records, an investigator is typically engaged in a race to obtain this electronic evidence once it is identified while concurrently juggling other matters on the investigation or on other cases.

Delay is an inherent part of the investigative process. Pursuing investigative leads and obtaining relevant information can take many months.[103] Requesting ECPA records is only one part of the investigative process which may include interviewing victims and witnesses, following financial leads, requesting and obtaining a search warrant for a business or residence, among many other steps.[104]

102. For further examples of the "electronic evidence lapse" problem, see *supra* Part II.B.

103. For example, as one congressional report noted, "[c]hild pornography investigations often take months to develop, during which time critical data, such as IP addresses linked to a subscriber's account, may be lost if the Internet Service Provider does not have an adequate retention policy." STAFF REPORT: SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET, *supra* note 20, at 4.

104. *See, e.g.*, United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007) (court affirmed conviction for a computer intrusion that was traced by a system administrator from

The process involves about ten discrete steps, as summarized below. In some cases, many of these steps may not consume much time. However, delay, which can occur at any step, may impact whether essential electronic records may be obtained for the investigation. The following review summarizes the key steps in the investigative process that law enforcement confronts in requesting initial records under ECPA.

1. *Step One*: Crime Reported; Investigation Opened; Initial Electronic Evidence Identified

An investigation commences upon the report of the crime. In opening the investigation, investigators may identify, or the crime victim may provide, initial information that confirms the existence of some Internet evidence that may relate to the crime. For example, the victim may provide an email account that was used in a fraud scheme or some communication that reveals an Internet Protocol address. Investigators will follow-up on this initial lead along with any others.

Delay Factors: Initially, a number of delay factors may affect whether law enforcement can obtain any electronic records based on the early identification of Internet evidence. For example, a fair amount of time may have passed between the time the crime occurred and was reported. Perhaps the victim originally did not realize that a crime had taken place. Since most records of Internet activity are available for a limited period, the longer the passage of time, the less likely the provider may have retained the records. If this is the only evidence law enforcement has to investigate the crime, the availability of it may be critical to identifying the perpetrator and/or solving the crime.[105] At this early juncture of the investigation, the availability of the electronic evidence remains unknown pending further legal process and receipt of the requested information from the provider.

---

one company to a university and then turned over to law enforcement. The defendant hacked into a computer system of Qualcomm Corporation in San Diego from computers at the University of Wisconsin).

105. For example, text messages, which are normally only retained for a couple of days at most, proved critical to solving a murder. *See House Hearings: Data Retention As a Tool for Investigating Internet Crimes*, *supra* note 27, at 16–17, 20–21 (statement of John M. Douglass, Chief Of Police, Overland Park, KS; Int'l Ass'n of Chiefs of Police, Alexandria, Virginia) (the unexpected preservation of text messages from the defendant's cell phone carrier along with other cell tower data turned out to be "the single most important piece of evidence in linking the defendant to the" murders of a 22-year old and her 10-month old son). In contrast, the unavailability of initial Internet evidence in other cases required closing the investigations. *See supra* Part Intro.C.2.

2. *Step Two*: Preservation Request Issued Under Section 2703(f)

Step two requires law enforcement to make a request under section 2703(f) to preserve information from the Internet evidence lead. This evidence may include, for example, an email address or an account connected to a particular Internet Protocol address.[106]

Before submitting the preservation request, the investigator will need to know where to send the request. This will involve identifying the provider maintaining the particular account. For example, the investigator may need to determine which provider is assigned the Internet Protocol address. Several initial questions may arise: Is it a common provider or one that is not well known, such as a provider furnishing proxy services?[107] Is the Internet Protocol address hosted in the United States or another country?[108] Once the provider for the account is identified, the preservation request will be sent and the information in the account will be preserved for 90 days pending receipt of legal process (with a possible extension for another 90 days).[109]

Frankly, this example is simplistic in that only one Internet evidence lead is being pursued. More commonly, for crimes committed over the Internet, multiple Internet leads may be available. For example, there may be multiple Internet Protocol addresses or email accounts that have been identified early in the investigation. A similar process to identify the host of the account and submit a preservation request must be made for each lead.

Some cases involve multiple victims. Each victim may have initial electronic evidence leads that need to be separately pursued following the same process. Investigators may need to review this evidence to determine whether the same perpetrator was involved or whether there are common threads.

Delay Factors: Initially, it may take law enforcement some time to identify the provider of the account. For example, law enforcement may need to determine which provider services the Internet Protocol address. If the address is from another country, a request will need to be made to law enforcement officials abroad.

A race is underway to preserve available account information. Whether any relevant information is in the account will not be known

106. For more on the preservation request process under 18 U.S.C. § 2703(f), see *supra* Part II.B.

107. For a description of proxy services see *infra* note 121.

108. For information on obtaining evidence in other countries, see *infra* text accompanying notes 130–36.

109. For a discussion concerning a preservation extension see *supra* note 98.

until legal process is prepared, submitted and the results are received. As already noted,[110] the mere request to preserve Internet records does not ensure they will be available. In some cases, even with a preservation request issued as soon as law enforcement learns about the account, no account records were available at the time of the request, requiring the case to be closed.[111]

If some time has passed before the crime was reported, there may be no relevant information remaining in the account at the time of the preservation request. If the perpetrator learns of the investigation, he or she may take steps to remove or delete the information. If this occurs before a preservation request can be submitted, there may be nothing left in the account after legal process is served. If so, this investigative lead and the time taken to pursue it will not yield meaningful investigative results to advance the investigation.

3. *Step Three*: Legal Process Prepared

With the preservation request submitted, law enforcement will begin preparing legal process. For example, for the content in the account, a search warrant may be prepared.[112] The investigator will want to take care to confirm the accuracy of the details in the affidavit before it is submitted to a judge.[113] This verification process will depend on the confirmation of other facts, either through witnesses or other records.

Probable cause is measured under the "totality of the circumstances."[114] The initial Internet lead (email address or Internet Protocol address) may be insufficient by itself to show probable cause. More likely, the agent will seek to include other information from the investigation to show probable cause. Additional information required for the affidavit may be pending other legal process. For example, the agent may be waiting for information about financial records in a financial crime that may be relevant or significant for the affidavit. Bank records can take several weeks to obtain from a financial institu-

110. *See supra* Part Intro.C.2.

111. *Id.* While this has occurred in a number of cases involving child pornography, see *supra* notes 55–56, the same principle applies to other crimes. If records for a key lead involving Internet evidence are unavailable, there may be no option but to close the case.

112. For more information, see *supra* note 99. Other process may include: a search warrant, court order, pen register or trap and trace order, or subpoena. *Id.*

113. *See* Franks v. Delaware, 438 U.S. 154 (1978) (a search's validity may be challenged if there are any material misstatements or omissions in the search warrant affidavit).

114. *See, e.g.*, Illinois v. Gates, 462 U.S. 213, 238 (1983) (adopting "totality of the circumstances" standard).

tion. The initial preservation request retains the information in the account, if any, for 90 days. However, given the need to obtain other information in the investigation and attend to other matters, the statute recognizes that an additional 90 days may be required to extend the initial preservation request.

During the preparation of legal process, the agent may seek guidance from the prosecutor to address legal or other issues in the case. Most prosecuting offices require that the prosecutor review the legal process before it is submitted to the court. Busy prosecutors will schedule time to address any issues and review the sufficiency of the legal process.

In preparing legal process, the time of the investigator will be divided among multiple demands and priorities. Concurrently, the investigator will be pursuing other leads in the case, such as interviewing other witnesses and pursuing financial records. The investigator will also be attending to other cases at the same time.

While the initial Internet lead has been preserved, significant new key leads may no longer be available by the time law enforcement learns of them. At this juncture, it remains unknown whether there will be an electronic evidence lapse for new leads.[115] This information will not be known until legal process is served and the results are returned.

Delay Factors: As noted, sufficient time will be needed to prepare the necessary legal process, including obtaining additional information, verifying the accuracy of information for an affidavit, or addressing legal issues with the prosecutor. The agent may be waiting for other information, such as bank records, before the affidavit can be completed. The time to prepare the legal process will depend on the circumstances of each case. Legal or other issues may need to be addressed with the prosecutor.

4. *Step Four*: Legal Process Submitted for Initial Review

After the legal process is completed, the agent submits the application for legal process to the court for initial review. Many federal judges, who are juggling time in court with other cases and demands, prefer to have a day or so to review the search warrant affidavit. If a judge is in trial or the middle of extended proceedings, the agent will typically drop off the legal process that will wait for the judge to review during a break or at the end of the day. The agent may be told to

115. For a discussion of the "electronic evidence lapse" problem see *supra* Part II.B.2.

return later in the day or the next day or so. Some courts today will accept the draft application by email. In some rural areas, the judge may not be readily available, as there may not be a full-time judge or the judge may be holding court in another part of the district.

During the period of initial review, the judge may have questions about the application for legal process. Modifications to the application may be required. Another day or so may be taken to confirm necessary information and prepare an updated affidavit or application to address the judge's questions.

Delay Factors: Even busy and hard-working courts considering many cases need time to review the final affidavit. Submitting the application or affidavit for judicial review can take a day or a couple of days or more.[116] Additional time may be spent responding to questions from the judge who may see issues that were not noted before. Modifications to the affidavit may be required, which will then be resubmitted for review. Where one day can make a difference, any delay can be consequential. Time is ticking on the availability of the fleeting electronic records for other accounts yet to be revealed during the ongoing investigation.

5. *Step Five*: Legal Process Formally Submitted to the Court

After the court has completed its initial review, if changes are required, a new affidavit must be submitted. The court will review the affidavit again.

If no questions arose during the initial review or no modifications were required, the investigator will be told to come to chambers. If the judge is in court proceedings, the investigator may wait at the courthouse until advised that the judge is ready to meet. For example, the investigator may wait until the judge comes off the bench on another matter. If the judge is in trial, the agent may be told to come at the end of the day or the next day during a break in the proceedings.

Delay Factors: Once the application is initially reviewed and ready to be completed, the agent will typically schedule an appointment or wait to meet with the judge. Where one day can make a difference, any delay can be consequential. Time keeps ticking on the availability of the fleeting electronic records for other accounts yet to be revealed during the ongoing investigation.

116. Steps four, five and six can occur on the same day or can take a couple of days or more, depending on the circumstances of the case and the availability of the judge. Busy judges have many priorities and cases that must be juggled concurrently.

6. *Step Six*: Legal Process Approved; Satisfaction of Oath Requirement

After being told to come to court, an agent will meet with the judge, normally in chambers. An application for a court order or search warrant is formally completed before the court. For example, normally for a search warrant, the affiant will swear under oath that the facts in the affidavit are accurate.[117] Once the application for a court order or search warrant is approved by the judge, it is normally filed under seal in the clerk's office.

Delay Factors: Normally an appointment is scheduled to meet personally with the judge who may be in court or attending to other cases and matters. In some larger western districts, investigators may need to drive several hours to get to the judge's chambers. Swearing a warrant can therefore take all day.

7. *Step Seven*: Legal Process Served or Executed on the Provider of the Account

Law enforcement serves or executes the legal process on the provider.[118] The provider then collects the information within the scope of the legal process (for example, if the search warrant approves communications during a particular period of time).

Delay Factor: Collection and provision of the information to law enforcement can range from about a week to a few weeks or even more. It remains to be seen whether any information remains in the account as requested at the time of preservation. Perhaps more significantly, time is ticking on the availability of electronic records for other accounts yet to be revealed during the ongoing investigation. By the time the information is received on the initial application, the retention period may have passed for new accounts that are identified later in the investigation.

117. While the search warrant will be submitted under ECPA, it will be prepared "using the [standard search warrant] procedures" under Rule 41 of the Federal Rules of Criminal Procedure. *See* 18 U.S.C. § 2703(a) (2006). The oath requirement is imposed by Rule 41(d)(2). *See* FED. R. CRIM. P. 41(d)(2).

118. Unlike a traditional search warrant under 18 U.S.C. § 3105, the investigator need not be present at the provider to serve or execute the ECPA search warrant. *See* 18 U.S.C. § 2703(g). Fax service is permitted. *Id.*

8. *Step Eight*: Provider Gives Information to Law Enforcement After Collecting Information Within the Scope of the Legal Process

Law enforcement receives the information from the provider. Questions may arise about the manner in which the provider maintains the records it provided. For example, questions may concern how the records provided are maintained or created including what events are memorialized. Records for providers often vary and record different events.

Delay Factors: Calls may be needed to the provider to address questions about the records.

9. *Step Nine*: Law Enforcement Review of Information

The information may be extensive or voluminous and may take some time for the investigator to review. The investigator may be able to corroborate the Internet records with other evidence obtained in the investigation, such as with financial records or witness interviews. New leads may result from the information, including the identification of new witness or accounts.

Delay Factors: Depending on how much information is provided, the investigator may need a fair amount of time to review and assess the information (the larger the amount of data that is provided, the larger amount of time to review it). The investigator may also learn that some records in the account were deleted or removed, which may require further questions be asked of the provider.

10. *Step Ten*: Pursue Investigation and Identify New Leads Based on Information Received from the Provider in Step (9)

The information from the provider may confirm who the primary perpetrators were or show that others were involved or more culpable. New evidence leads may also be identified, such as the use of other email accounts or Internet Protocol addresses.

On the new leads, it will remain to be seen whether the investigators will confront the electronic evidence lapse problem.[119] The investigator will have to pursue the same steps described above for the new leads. If a sufficient amount of time has passed since the original Internet evidence lead, requests to preserve the new Internet evidence leads may be too late to protect the evidence.

119. For a discussion of the "electronic evidence lapse" problem see *supra* Part II.B.2.

Delay Factors: New accounts and leads may have been created around the time of the incident but, due to the passage of time, may not have been retained by other providers. Whether information is retained will not be known until legal process is submitted and the results are received.

11. Summary: Challenges in Identifying, Preserving, Requesting and Obtaining Electronic Evidence

As the steps to obtain ECPA records demonstrate, a fair amount of time can be taken to identify, preserve, request and receive the electronic records. Delays may occur at each step in the process. Time typically makes all the difference in obtaining the evidence or in determining whether new leads can be discovered and pursued. Law enforcement must race to obtain the fleeting information before the retention period lapses and must act as soon as new leads are developed.

The foregoing example is a fairly straightforward one involving a request for information based on one lead and information provided by the victim.[120] For many Internet crimes, comparable leads are being pursued for multiple providers at the same time. The next part highlights the complication where proxies or redirection efforts are undertaken by the defendant.

D. Acts to Conceal Criminal Activity: Use of Proxy, Redirection or Concealment Tools

In contrast to the foregoing straightforward example involving only one account, in most cases the process of collecting Internet evidence is more extensive and time consuming. Usually pursuing investigative steps is much more complicated, particularly when sophisticated criminals seeking to evade detection by law enforcement are involved. A number of tools can be used to conceal the perpetrators or to make it appear that someone else may be responsible for the criminal activity.

120. For another example of similar straightforward investigative facts which led to the identification of the defendant, see *Trotter* where the court affirmed a section 1030(a)(5) conviction for hacking into the Salvation Army computer network and noted that the "investigation discovered the intrusions into the Salvation Army's network originated from a DSL account in St. Louis, Missouri, registered to . . . Trotter's girlfriend and co-habitant" and that the "email address attached to the account included Trotter's first name, last initial, and birth year." United States v. Trotter, 478 F.3d 918, 920 (8th Cir. 2007). Most cases are much more involved and time-consuming in following the electronic evidence leads.

Building on the investigative facts above, assume that the defendant used a proxy or took steps to deliberately "bounce" through other internet locations as part of an effort to conceal the source of the Internet activity.[121] Each connection will take time to determine who holds the records at the proxy or jump off point. At the end of the sequence, the final provider may no longer retain the records that confirm who committed the offense or that show how the offense was committed.

The provider for the victim's computer checks the access logs to determine what the Internet Protocol address was for the last computer making a connection. The provider is unable to determine the source of the Internet activity and can only look to the last computer connecting with the victim's account.

The following summary demonstrates these challenges building on the prior steps.

1. Discovery of Access Through Another Site or Location

Building on the example above, assume in step nine that law enforcement received information from the provider based on the initial Internet evidence (such as an Internet Protocol address).[122] The information from the first provider reveals that the account access was actually made through another site by a particular Internet Protocol address (which will later be confirmed to be a proxy site).

As related in step two above, law enforcement will make a request under section 2703(f) to preserve information from the new Internet evidence lead. The same steps (3 through 9) will be followed to pre-

121. A "proxy" provides a "middleman" connection on the Internet. The use of the proxy conceals the original Internet Protocol address of the user requesting the information. *See* GLOSSARY OF SECURITY TERMS, *supra* note 4, at 146 (defining "proxy" as "an application that 'breaks' the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network").

An example of the redirection of Internet activity abroad to conceal domestic activity can be found in the CAN-SPAM Act prosecution in *Kilbride*. *See* United States v. Kilbride, 584 F.3d 1240 (9th Cir. 2009) (affirming convictions). Trial evidence showed that the defendants "arranged to remotely log on to servers in Amsterdam, to make it look like their spam messages were being sent from abroad, when in reality Kilbride and Schaffer were operating their business from inside the United States." Press Release, U.S. Dep't of Justice, Jury Convicts Two Men for Running International Pornographic Spamming Business (June 25, 2007), *available at* http://www.justice.gov/opa/pr/2007/June/07_crm_453.html.

122. *See supra* Part II.C.9.

pare and submit legal process for approval to the court and then submit the legal process to the provider. At this juncture, it is unknown whether there will be an electronic evidence lapse in the newly identified Internet lead.[123] In other words, given the limited retention period on the Internet records, the time taken to obtain and pursue the initial Internet evidence lead may exceed the retention period for the newly discovered lead. The lapse in the new records may require closing the investigation. Whether any relevant information is in the account will not be known until legal process is pursued and the provider gives the information to law enforcement.

2. Tracing the Use of Multiple Proxies

Building on this basic example, let's turn to a more realistic one. Assume that the defendant (E) took extra steps to conceal Internet activity by using three proxies (B, C, and D) to connect to the victim's computer (A). In the following Proxy Diagram, assume the following Internet Protocol addresses for each computer were used:[124]

Proxy Diagram:

Victim (A)	Third Proxy (B)	Second Proxy (C)	First Proxy (D)	Defendant (E)
12.34.56.77	34.56.78.99	56.78.90.11	78.90.12.33	11.22.33.44

Starting with the victim's computer or account (A), law enforcement will have to trace each connection, using the steps in the Diagram, provider by provider (B then C then D), to determine the original Internet transmission source (E) (defendant). For example, law enforcement will first determine who was the provider and account holder for computer (B) using IP Address 34.56.78.99 (listed as Third Proxy) to connect with the victim (who was using computer (A) (victim computer) and IP Address 12.34.56.77) at the date and time of the crime. Initially, questions may focus on whether the crime was committed by the user of computer (B) (third proxy) since it made the connection to the victim's account. At this point, it is not known whether computer (B) is the final link in the chain.

123. For a discussion of the "electronic evidence lapse" problem see *supra* Part II.B.2.

124. Instead of using a proxy, the defendant could hack into a series of computer networks before connecting to the victim's computer or account to disguise the source of the Internet activity. The same investigative steps would be followed.

By following the steps in the Proxy Diagram above, in the event that the provider for computer (B) (IP Address 34.56.78.99) has retained this information, law enforcement will learn for the first time that at the same date and time of the access to the victim's computer or account (A), the Internet communication or transmission was made through another account (C) (here Second Proxy) through IP Address 56.78.90.11. These records now confirm that no one using computer or network (B) was responsible for the crime. In this manner, the electronic records exclude an initial suspect or lead. Instead, computer (B) was used as a proxy (here third proxy). New questions arise. Did computer (C) initiate the crime or was it also used as a proxy?

If the provider for computer (B) (IP Address 34.56.78.99) did not retain the information about the access, then the investigation cannot proceed. Unless there is other independent evidence, this investigation may be closed. The victim will have no remedy in the criminal justice process.

Assuming that the provider for computer (B) (IP Address 34.56.78.99) retained the necessary records, once again, law enforcement will seek to learn the identity of the provider and account holder for this computer (C) using this IP Address at this time. Legal process will be pursued. If the records are retained, law enforcement will learn about the existence of computer (D) (here, the first proxy using IP Address 78.90.12.33). As legal process is obtained to identify the provider and user of IP Address 78.90.12.33 at the date and time of the crime, it remains unknown whether there are more links and proxies in the chain. In the event that the provider for computer (D) (IP Address 78.90.12.33) retained the necessary records, law enforcement will learn about computer (E) using IP Address 11.22.33.44, which turns out to be the defendant's computer. With this information, law enforcement may obtain a search warrant for the computer used by the defendant. If the records have not been removed or deleted, law enforcement may be able to connect the user, the defendant, to the unauthorized access to the victim through the first, second and third proxies.

This process can consume a substantial amount of time. When the crime was first reported, it was unknown whether or how many proxy computers may have been used. Only if each provider has retained the Internet access and other records will the crime be solved. The number of proxies (or links between computers) will be unknown until the final destination is identified.

This example, which is fairly straightforward, demonstrates the challenges that law enforcement confronts in seeking to obtain Internet records to confirm the unauthorized access of the victims computer (A). If the records are retained at four providers, law enforcement may be able to solve the crime. If not, unless other independent evidence is available, the investigation may be closed.

One more realistic update: assume that the use of the proxies is not linear (from E to D to C to B to A). Instead, the defendant jumbles the use of the proxies by using some proxies more than once (such as from E to D to B to C to D to B to C to A). Law enforcement will have to trace each link. With more links, the risk of an electronic evidence lapse increases.

3. Summary

These examples demonstrate that identifying, requesting and obtaining electronic records involves a race against time and many discrete steps along the way. The mere preservation alone does not ensure that necessary electronic evidence from the Internet will be available. There are many steps in the process that may result in delay. Even if the initial Internet evidence lead is preserved and obtained by law enforcement, new leads may be unavailable as a result of the electronic evidence lapse. A longer retention period enhances the likelihood that necessary evidence may be available for law enforcement use. None of the records will be provided unless law enforcement submits sufficient legal process.

E. Division of Criminal Labor

Another complicating factor in cracking criminal conspiracies is the division of labor that may be used to commit the crime.[125] This division of labor is common for more sophisticated crimes. The challenge for law enforcement is that the criminal actors and evidence of crimes committed on the Internet may be in many different jurisdictions.

For example, in trade secret prosecutions, it is not uncommon for a trusted insider with access to the information to misappropriate or steal the trade secret. This individual usually has technical and specialized skills to develop the trade secret. However, he usually lacks the skills and ability to develop, manufacture or market the misappro-

125. As an example, a division of labor normally occurs in a conspiracy where each defendant contributes different skills or steps to further the crime.

priated trade secret. Others with these skills may be invited to join the conspiracy. The evidence trail showing preparation, planning, misappropriation and use among these participants will typically be scattered in multiple locations.

As another example, in an online fraud case:

> [T]he tasks of [1] writing code, [2] locating hosts for phishing sites, [3] spamming, and [4] other components of a full-scale phishing operation may be divided among people in various locations. This means that in some phishing investigations, timely cooperation between law enforcement agencies in multiple countries may be necessary for tracing, identification, and apprehension of the criminals behind the scheme.[126]

In a criminal copyright prosecution involving the unlawful distribution of copyrighted works on the Internet, the division of labor included:

> Higher level members of the warez groups, known as site operators or "SiteOps," [who] administered and maintained the site and controlled access to the site by use of security measures such as usernames and passwords. Others serve as "equipment suppliers" (providing hardware (such as hard drives, computer parts, and computer servers) to the warez site), "encoders" or "crackers" (those defeating copy protection devices); "scripters" (creating, programming, and helping build the warez site); "brokers" (who found groups to participate on the warez site). Lower level members included "suppliers" (providing an unauthorized copyrighted movie, game or software), "cammers" (those making unauthorized camcorder recordings in movie theaters), "couriers."[127]

This division of labor may require law enforcement to coordinate with partners in other jurisdictions. The race to obtain Internet evidence is thus further complicated.

F. Multi-Jurisdictional, International Issues

Another race involves gathering evidence in other countries. Given the global reach of the Internet, it is not uncommon for evidence of the crime to be in another country. For example, "phishing" cases may involve individuals who organize and plan the scheme in different countries.[128]

126. REPORT ON PHISHING, *supra* note 1, at 11.

127. *See* Press Release, U.S. Dep't of Justice, Five Additional Defendants Charged with Violating Copyright Laws as Part of Operation Copycat (April 6, 2006), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2006/soaresCharge.htm. The authors prosecuted "Operation Copycat" during their tenure in the U.S. Attorney's Office in the Northern District of California.

128. *See, e.g.*, REPORT ON PHISHING, *supra* note 1, at 11 (noting concern that "full-fledged criminal organizations in various countries" were organizing "to conduct phishing

Another potential source of delay may result from obtaining electronic or other evidence maintained in other countries. While established procedures facilitate requests for assistance in other countries, the process takes longer than a domestic request.[129] As noted below, among other requirements, the legal requests must be translated into the language of the country where the evidence is located before the request may be submitted.

The U.S. Department of Justice, Office of International Affairs ("OIA") coordinates requests for evidence with their counterparts in other countries. Normally, the request must be submitted through either a Mutual Legal Assistance Treaty ("MLAT"),[130] or letter rogatory.[131] The requests must be translated into the language of the country in which assistance is sought.[132]

An MLAT request is based upon a treaty between countries which sets forth the process and circumstances in which one country may request evidence for a criminal case which is maintained in another country.[133] The law enforcement request may include identifying subscriber account information, obtaining witness interviews or deposi-

schemes on a systematic basis" premised on "indications that criminal groups in Europe are hiring or contracting with hackers to produce phishing e-mails and websites and develop malicious code for use in phishing attacks."); Operation Phish Phry, *supra* note 13 (providing a case example of this approach).

129. *See House Hearings: Data Retention As a Tool for Investigating Internet Crimes*, *supra* note 27, at 70–71 (statement of Jason Weinstein, Deputy Assistant Att'y Gen. of the United States) (describing a multinational law enforcement operation which took law enforcement officials in Australia and the United States two years to rescue a girl in Georgia after videos of her being abused were distributed on the Internet); *see also* Robin Bowles, *In Harms Way: Australian police played a key role in finding a young girl at the mercy of a brutal pedophile*, SYDNEY MORNING HERALD, July 25, 2009, *available at* http://www.smh.com.au/national/in-harms-way-20090724-dw6l.html (describing international investigation and assistance by Australian law enforcement).

130. *See generally* U.S. DEP'T OF JUSTICE, UNITED STATES ATTORNEY'S MANUAL, CRIMINAL RESOURCE MANUAL 276 (1997) [hereinafter CRIMINAL RESOURCE MANUAL], *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00276.htm (describing the process for handling treaty requests).

131. *See generally* CRIMINAL RESOURCE MANUAL, *supra* note 130, at 275, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00275.htm (describing the process for handling a letter rogatory).

132. *See* 28 U.S.C. § 1781 (2006) (transmittal of letter rogatory or request); *id.* § 1782 (assistance to foreign and international tribunals and to litigants before such tribunals). *See generally* CRIMINAL RESOURCE MANUAL, *supra* note 130, at 282, *available at* http://www.justice.gov/ usao/eousa/foia_reading_room/usam/title9/crm00282.htm#282 (noting requirement of translations).

133. *See, e.g.*, Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Fr., Dec. 10, 1998, S. TREATY DOC. No. 106-17 (2000), *available at* http://www.state.gov/documents/ organization/121413.pdf.

tions or testimony,[134] seizure of records and evidence, certification of foreign business records,[135] forfeiture of assets, and other law enforcement steps. In the absence of an MLAT, a letter rogatory must be submitted by a judge who makes a formal request to the judiciary of another country. While electronic records may be preserved if the country in which the evidence is located is a member of the 24/7 Cyber Network, the request preserves existing records pending completion of the MLAT process.[136]

G. Summary

These examples are only a few among many others. They illustrate the inevitable delay that is inherent in the process of obtaining electronic records for a criminal investigation. As these examples show, law enforcement is constantly racing against clock to obtain electronic records from providers. Delay is inherent and inevitable in the process. Despite the best and prompt efforts of law enforcement, whether the necessary Internet records are available may turn on the retention policies of the provider.

III. Legislative Proposals Imposing New, Higher Standards Under ECPA Fail to Consider and Address the Resulting Delays for Law Enforcement in Obtaining Fleeting Internet Records

Recent efforts have been advanced to amend ECPA, including the Stored Communications Act.[137] Some of the proposed ECPA amendments would impose new and higher standards to obtain elec-

134. Rule 15 of the Federal Rules of Criminal Procedure may be used to obtain the deposition of "a prospective witness . . . in order to preserve testimony for trial." FED. R. CRIM. P. 15.

135. Foreign business records may be admitted under the certification requirements. 18 U.S.C. § 3505 (foreign records of regularly conducted activity); *see also generally* United States v. Hagege, 437 F.3d 943, 956 (9th Cir. 2006) (admitting foreign bank records from Luxembourg and Israel under section 3505).

136. Council of Europe: Convention on Cybercrime, art. 35 (Nov. 23, 2001) E.T.S. No. 185 (establishing the Council of Europe 24/7 Network), *available at* http://conventions.coe.int/Treaty/en/Treaties/html/185.htm; *see also* Sergio Staro, *The G8 24/7 Network* (May 13, 2010), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/presentations/Regional%20Ws%20on%20Cybercrime_13May10/2215_The_G8_24-7%20Network_SStaro.pdf (describing the operation of the 24/7 Network). The Council of Europe's Cybercrime Convention is an example of how the international community came together to address the practical realities recognizing the need to obtain electronic evidence in other countries.

137. *See, e.g.*, Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011); ECPA 2.0 Act of 2012, H.R. 6529, 112th Cong. (2012).

tronic evidence and records.[138] None of these proposals considers or addresses the impact of new delays that would result from the higher standards for law enforcement to obtain electronic records.

While we leave to policymakers the task of determining the merits of such proposals, part of the debate should recognize that adding further delay to an already burdensome process would result in less information being available to law enforcement from the trail of Internet evidence. The evidence involves information that the defendant voluntarily provided to third party Internet providers while the crime was being committed.

Any serious proposal should explicitly answer the question of how much longer law enforcement would be delayed in obtaining Internet records under the proposed new standards. The proposals should also consider how the "electronic record lapse" problem would be addressed. The public policy consequence of further delay will result in the inability of law enforcement to solve crimes in which Internet evidence may be vital. Many examples have been noted in which crimes were solved based on electronic records.[139]

As part of this public policy debate, to the extent that further delay would result from any legislative proposals, the greater need for mandatory retention policies must be considered. Only by ensuring that the records are retained and available to law enforcement upon sufficient legal process can the legitimate needs of law enforcement be met.

IV. Moving Toward Longer Retention Policies

Steps to increase the retention of Internet-based records will better ensure that key evidence may be available to prove the crime. The

138. *See The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. (2011) (statement of James A. Baker, Assoc. Deputy Att'y Gen. of the U.S.), *available at* http://www.fas.org/irp/congress/ 2011_hr/ecpa.pdf (in considering amendments to ECPA, "what we must not do—either intentionally or unintentionally—is unnecessarily hinder the Government's ability to effectively and efficiently enforce the criminal law and protect national security. The Government's ability to access, review, analyze, and act promptly upon the communications of criminals that we lawfully acquire, as well as data pertaining to such communications, is vital to our mission to protect the public from terrorists, spies, organized criminals, kidnappers, and other malicious actors. At the Department of Justice, we are prepared to consider reasonable proposals to update the statute—and indeed, as set forth in my written statement for the record, we have a few of our own to suggest—provided that they do not compromise our ability to protect the public from the real threats that we face.").

139. *See supra* Part Intro.A.1–2 (providing examples of crime involving the Internet).

records would not be provided unless law enforcement could make the requisite showing to obtain legal process. For example, the contents of communications may be obtained with a search warrant under present law.[140]

Over the past decade and a half, senior law enforcement officials and members of Congress have suggested a national retention policy may be needed. Most of the discussion has occurred concerning how to best combat the sexual exploitation of children, however, the same concerns and steps are involved in investigating other crimes.

A. Voluntary Steps by Industry Should Be Considered

Ideally, voluntary industry steps to retain key electronic records should be promoted. Some providers have indicated a willingness to establish a longer period of retention for selected Internet records[141] and some members of Congress have strongly suggested that industry take the lead in this area.[142] This suggests that industry may be able to develop appropriate retention standards without a mandatory requirement imposed under law. If so, these voluntary steps should be encouraged. Of course, core questions will remain, specifically what records should be retained and for how long?

140. 18 U.S.C. § 2703(a).

141. *E.g.*, *House Hearings: Making the Internet Safe*, *supra* note 94, at 95 (statement of Tom Daily, General Counsel, Verizon Communications) ("While the debate over data retention is still forming, Verizon's general view is that IP address assignment and customer record information collected in the normal course of business could be retained by network providers for a reasonable period of time, and if retention is required, that the period of retention should be long enough reasonably to enable law enforcement to conduct their investigations. Whether this obligation should extend to others in the Internet community is still open to debate, as is whether the period of retention should be 24 months (as has been proposed) or a shorter period more in line with the retention policies of businesses in effect today."); *see also, e.g.*, *id.* at 96 (statement of Jerry Lewis, Vice President, Deputy General Counsel, and the Chief Privacy Officer of Comcast) ("Because of the importance of child safety, we want to do more. We have decided to extend our retention of IP address assignment information to 180 days.").

142. *See House Hearings: Data Retention As a Tool for Investigating Internet Crimes*, *supra* note 27, at 65 (statement of Rep. Deborah Wasserman Schultz) ("Voluntarily would be a lot better than mandating this. I think that is what we would all like to see, including law enforcement."); *id.* at 74–75 (statement of Rep. Tom Marino) ("So I implore you, please regulate this to the extent where it is effective and efficient yourselves because, I can agree with the Chairman and my colleagues, at one point, we will step in.").

B. Past Executive Branch and Law Enforcement Support for Data Retention Standards

For more than a dozen years, executive branch officials in the Department of Justice and the Federal Bureau of Investigation have supported longer retention periods for electronic evidence. While much of the discussion concerns child exploitation cases, the same hurdles apply to other Internet-based offenses.

In 1999, then-Deputy Attorney General Eric H. Holder, Jr., supported data retention by ISPs.[143] At an international conference, he recommended: "we must take steps to ensure that we can obtain the evidence necessary to identify child pornographers. That means certain data must be retained by ISPs for reasonable periods of time so that it can be accessible to law enforcement."[144]

In 2006 Senate committee testimony, Attorney General Alberto R. Gonzales suggested that the retention of records was important in child exploitation cases:

> As we've looked at ways to improve the law enforcement response to the problem of online exploitation and abuse of children, one thing we've continuously heard from state and local investigators and prosecutors is that many Internet Service Providers don't retain records for a sufficient period of time. Several months ago, I asked a working group within the Department to look at this issue, and we're working hard on ways to remedy this problem.[145]

143. *See infra* note 144 and accompanying text.

144. Eric Holder, Deputy Att'y Gen. of the U.S., Remarks at the International Conference on Combating Child Pornography on the Internet (Sept. 29, 1999) (transcript on file with the University of San Francisco Law Review); *see also* Declan McCullagh, *Obama's Attorney General Pick: Good on Privacy?*, CNET NEWS (Dec. 2, 2008), http://news.cnet.com/8301-13578_3-10110922-38.html (noting comments from 1999).

145. *Combating Child Pornography by Eliminating Pornographers' Access to the Financial Payment System: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 109th Cong. 9 (2006) [hereinafter *Combating Child Pornography*] (statement of Alberto R. Gonzales, Att'y Gen. of the United States), *available at* http://banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=53efb328-0d12-4eb9-a1df-eaaf502be49d; *see also* Alberto R. Gonzales, Att'y Gen. of the U.S., Remarks at the National Center for Missing and Exploited Children (April 20, 2006), *available at* http://www.justice.gov/archive/ag/speeches/2006/ag_speech_060420.html ("The investigation and prosecution of child predators depends critically on the availability of evidence that is often in the hands of Internet service providers. This evidence will be available for us to use only if the providers retain the records for a reasonable amount of time. Unfortunately, the failure of some Internet service providers to keep records has hampered our ability to conduct investigations in this area. As a result, I have asked the appropriate experts at the Department to examine this issue and provide me with proposed recommendations. And I will reach out personally to the CEOs of the leading service providers, and to other industry leaders, to solicit their input and assistance. Record retention by Internet service providers consistent with the legitimate privacy rights of Americans is an issue that must be addressed."); Anne Broache, *U.S. Attorney Gen-*

In 2008, during oversight hearings, FBI Director Robert S. Mueller, III, agreed that a two-year retention period for Internet Service Providers was appropriate and consistent with other countries:

> Mr. [RIC] KELLER. Is the challenge them [Internet Service Providers] not cooperating or them not keeping their records long enough?
> Mr. MUELLER. It is a question of having a standard against which you retain the records. The European Union has a standard now for ISPs that generally can go up to 2 years. And some of the concerns are the storage. Some of the concerns are developing the software that would allow you to keep the requisite records.
> But from the perspective of an investigator, having that backlog of records would be tremendously important if somebody comes up on your screen now and you want to know and make the case as to the past activity of that individual. If those records are only kept 15 days or 30 days, you may lose the information you need to be able to bring the person to justice.
> Mr. KELLER. Are you suggesting a 2-year guideline comparable to other countries?
> Mr. MUELLER. I believe that would be helpful, yes.[146]

During congressional hearings in 2011, the Department of Justice underscored its continued support for data retention standards in order to address law enforcement needs. Deputy Assistant Attorney General Jason Weinstein testified:

> Currently, despite the diligent and efficient work by law enforcement officers at all levels, critical data has too often been deleted by providers before law enforcement can obtain that lawful process. This gap between providers' retention practices and the

eral Calls for 'Reasonable' Data Retention, CNET NEWS (Apr. 20, 2006), http://news.cnet.com/U.S.-attorney-general-calls-for-reasonable-data-retention/2100-1030_3-6063185.html ("'Record retention by Internet service providers (that is) consistent with the legitimate privacy rights of Americans is an issue that must be addressed.'"); Declan McCullagh, *Gonzales pressures ISPs on data retention*, CNET News (May 26, 2006), http://news.cnet.com/Gonzales-pressures-ISPs-on-data-retention/2100-1028_3-6077654.html?tag=contentMain;contentBody;1n ("U.S. Attorney General Alberto Gonzales and FBI Director Robert Mueller on Friday urged telecommunications officials to record their customers' Internet activities . . . .").

146. *Oversight of the Federal Bureau of Investigation: Hearing Before the H. Comm. on the Judiciary*, 110th Cong. 54 (2008) (statement of Robert S. Mueller, III, Director, Federal Bureau of Investigation), *available at* http://judiciary.house.gov/hearings/printers/110th/41904.pdf; *see also id.* at 37 ("[R]ecords retention by ISPs would be tremendously helpful in giving us the historical basis to make a case in a number of these child predators who utilize the Internet to either push their pornography or to lure persons in order to meet them."); *id.* at 75 (noting "that records retention would be of assistance in terms of addressing these problems"); Declan McCullagh, *FBI, Politicos Renew Push for ISP Data Retention Laws*, CNET NEWS (Apr. 23, 2008), http://news.cnet.com/8301-13578_3-9926803-38.html ("FBI Director Robert Mueller told a House of Representatives committee that Internet service providers should be required to keep records of users' activities for two years.").

> needs of law enforcement can be extremely harmful to investigations that are critical to protecting the public from predators and other criminals.. . .
>
> In short, the lack of adequate, uniform and consistent data retention policies threatens our ability to use the legal tools Congress has provided to law enforcement to protect public safety.[147]

More recently, on September 19, 2012, Assistant Attorney General Lanny A. Breuer, Assistant Attorney General for the Criminal Division in the U.S. Department of Justice, noted the impact on solving complex cybercrime of the inability to obtain electronic evidence from providers. As he framed the challenge:

> The lack of data retention by ISPs and other providers is a serious problem and one that many within and outside the Department of Justice have recognized. Today's cybercriminals are more sophisticated than ever. They use botnets, proxy servers and other methods to hide their true identities. To track them down, we often need to follow an electronic trail, frequently around the globe, and that usually means obtaining a search warrant or other legal process to gain access to critical online data. To the extent that following such trails is made more difficult—because the legal standards become more stringent, or because ISPs delete the data too quickly—our job as law enforcement officers will also become more difficult.[148]

Other law enforcement groups have urged the adoption of retention policies. For example, in 2006, 49 state attorneys general wrote a letter to congressional leaders urging Congress to move toward a federal solution on data retention that would meet the needs of law enforcement and privacy concerns. The letter noted:

> Because ISPs are often national, if not global businesses, data retention requirements are better suited for federal legislation than state legislation that may vary by jurisdiction; a position supported by the National Center for Missing and Exploited Children. Accordingly, we call on Congress to dedicate the resources necessary to study this issue and to implement a meaningful national standard for ISP data retention that provides law enforcement with the tools necessary to combat the spread of internet-based crimes against children. In doing so, we encourage you to work with law enforcement at all levels of government and the ISP industry itself,

147. *House Hearings: Data Retention as a Tool for Investigating Internet Crimes*, *supra* note 27, at 7; *see also id.* at 47–48 (suggesting that a data retention requirement should "apply to all crimes not just to child exploitation").

148. Lanny A. Breuer, Assistant Att'y Gen., Speech at Fordham University School of Law (Sept. 19, 2012), *available at* http://www.justice.gov/criminal/pr/speeches/2012/crm-speech-120919.html.

> and to adopt a standard that respects the legitimate privacy rights of citizens.[149]

Also in 2006, the International Association of Chiefs of Police ("IACP") adopted a resolution urging adoption of a uniform data retention standard. Among other findings, the resolution noted:

> [T]he failure of the Internet access provider industry to retain subscriber information and source or destination information for any uniform, predictable, reasonable period has resulted in the absence of data, which has become a significant hindrance and even an obstacle in certain investigations, such as computer intrusion investigations and child obscenity and exploitation investigations, although law enforcement has generally acted expeditiously in processing lawful requests to Internet providers.[150]

The resolution provided:

> RESOLVED that the IACP strongly urges national legislatures, the Internet administration and telephony communities, including regional Internet registries, the Internet Corporation for Assigned Names and Numbers, domain-name registries, domain-name registrars, Internet access and service providers, and telecommunication providers, to develop an appropriate but uniform data retention mandate for both the aforementioned Internet administration community and telephony service providers requiring the retention of customer subscriber information and source and destination information for a minimum specified reasonable period of time so that it will be available to the law enforcement community, upon applicable legal process, to enhance public safety and prevent, deter, or detect terrorists and criminals through the ability to investigate offenses facilitate by use of the Internet and telephony . . .[151]

These examples demonstrate a continuing interest by the highest officials in federal law enforcement and others for a national data retention requirement. Law enforcement support for data retention has been highlighted for more than a dozen years.

---

149. *See* Letter from 49 State Attorneys General to Congress (June 21, 2006), *available at* http://www.naag.org/assets/files/pdf/signons/20060622.dr-letter-final.pdf. In a transition paper for the new Obama Administration, the National Association of Attorneys General listed the issue of mandating data retention standards. *See* NAT'L ASS'N OF ATT'YS GEN., INTERIM BRIEFING PAPER, PREPARED FOR: PRESIDENT-ELECT BARACK OBAMA TRANSITION TEAM (2009), *available at* http://otrans.3cdn.net/20ef0c0e1525cbf366_gpvm6gcxo.pdf.

150. INT'L ASS'N OF CHIEFS OF POLICE, 2006 RESOLUTIONS: SUPPORT FOR DATA RETENTION IN AID OF THE INVESTIGATION OF CRIMES FACILITATED OR COMMITTED THROUGH THE USE OF THE INTERNET AND TELEPHONY-BASED COMMUNICATIONS SERVICES 45 (2006) (adopted at the 113th Annual Conference), *available at* http:// www.theiacp.org/resolution/2006Resolutions.pdf.

151. *Id.* at 46.

C. Recent Legislative Support and Legislation

Some members of Congress have also voiced support for data retention standards. A congressional staff report suggested that consideration should be given to mandate that Internet Service Providers retain "IP address information linked to subscriber information."[152] Over the past few congresses, legislation has been introduced which would require data retention.

1. Current Congress: 112th Congress

In the current Congress, legislation has been reported out of committee and is pending for consideration by the House of Representatives. On May 25, 2011, House Judiciary Committee Chairman Lamar Smith (R-Texas) and Congresswoman Debbie Wasserman Schultz (D-Florida) introduced H.R. 1981, the Protecting Children From Internet Pornographers Act of 2011.[153] On July 12, 2011, hearings were held before the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security. Chairman Smith testified that the retention provision was based on a comparable Federal Communications Commission standard for telephone records:

> H.R. 1981 directs Internet service providers to retain Internet protocol addresses to assist Federal law enforcement officials with child pornography and other Internet investigations. This is a narrow provision that addresses the retention of only the Internet protocol addresses that providers assign to their customers. It does not require the retention of any content. So the bill does not read any legitimate privacy interests of the Internet users. . . . H.R. 1981 requires providers to retain these records for 18 months. This mirrors an existing FCC regulation that requires telephone companies to retain for 18 months all toll records, including the name, address, and telephone number of the caller, plus each telephone number called and the date, time, and length of the call. In effect, this bill merely applies to the Internet what has applied to telephones for decades.[154]

152. STAFF REPORT: SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET, *supra* note 20, at 4 ("Due to the fact that harm may be occurring to a child in real-time during an investigation involving the sexual exploitation of children over the Internet, Congress should consider requiring ISPs that provide connectivity to the Internet to retain such IP address information linked to subscriber information necessary to allow law enforcement agents to identify the IP address being used to download or transmit child pornography images and only for so long as necessary to accomplish that purpose.").

153. Protecting Children From Internet Pornographers Act of 2011, H.R. 1981, 112th Cong. (2011).

154. *House Hearing: Protecting Children*, *supra* note 57, at 16 (referring to 47 C.F.R. § 42.6 (1986)) ("Each carrier that offers or bills toll telephone service shall retain for a period of 18 months such records as are necessary to provide the following billing information about

House Judiciary Subcommittee member, Congresswoman Sheila Jackson Lee (D-Texas), framed the issue as trying to balance different interests: "at [the] crux of this issue is determining a balance between the necessary amount of data retention which would best serve law enforcement, the impact of added retention costs on providers, and the looming privacy concerns of the majority of law abiding Internet users."[155]

The House Judiciary Committee reported out the measure, as amended, on December 9, 2011. The bill remains pending for consideration by the House of Representatives.[156] As reported, the retention period was reduced to "a period of at least one year" and would apply to a "commercial provider of an electronic communication service" requiring retention of "a log of the temporarily assigned network addresses the provider assigns to a subscriber to or customer of such service that enables the identification of the corresponding customer or subscriber information."[157] The measure provides a "Sense of Congress" that records "should be stored securely to protect customer privacy and prevent against breaches of the records."[158] The retention period is not limited to child pornography cases and applies to all data. Given higher costs in retaining data, the measure eliminates a private right of action against the provider, available under current law, for disclosing information to law enforcement.[159]

Identical legislation has been introduced in the Senate. On June 30, 2011, Senator Orin Hatch (R-Utah) introduced S. 1308, entitled Protecting Children From Internet Pornographers Act of 2011, with Senator Amy Klobuchar (D-Minnesota) and Senator Marco Rubio (R-Florida).[160] The measure also proposed an 18-month retention period of "a log of the temporarily assigned network addresses that the ser-

telephone toll calls: the name, address, and telephone number of the caller, telephone number called, date, time and length of the call. Each carrier shall retain this information for toll calls that it bills whether it is billing its own toll service customers for toll calls or billing customers for another carrier.").

155. *Id.* at 81; *see also id.* at 42–43 (statement of Marc Rotenberg, President, Electronic Privacy Information Center) (raising concerns about the impact on privacy).

156. H.R. Rep. No. 112-281, pt. 1 (2011).

157. *See* H.R. 1981; H.R. REP. NO. 112-281, at 22 (amendment to narrow the retention period to 180 days was defeated by a vote of 12 to 14); *id.* at 50 n.40 (a one-year period was adopted by a manager's amendment to the bill).

158. *See* H.R. 1981, § 4(b).

159. *Id.* § 5.

160. Protecting Children From Internet Pornographers, S. 1308, 112th Cong. (2011); *see also* 157 CONG. REC. S4294 (daily ed. June 30, 2011) (statement of Sen. Orrin Hatch upon introduction noting "this bill requires companies such as Internet service providers to retain information such as subscriber network addresses for at least 18 months . . . The

vice provider assigns to each subscriber account, unless that address is transmitted by radio communication."[161]

2. Prior Congress: 111th Congress

In the prior Congress, Senator John Cornyn (R-Texas) introduced S. 436, 111th Cong., 1st Sess. (Feb. 13, 2009), entitled the "Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act of 2009" or the "SAFETY Act." The measure provided: "A provider of an electronic communication service or remote computing service shall retain for a period of at least two years all records or other information pertaining to the identity of a user of a temporarily assigned network address the service assigns to that user."[162] On the same day, Congressman Lamar Smith (R-Texas) introduced a companion bill in the House, H.R. 1076 111th Cong., 1st Sess. (Feb. 13, 2009), the "Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act." The same retention period and provision was included in the House bill.[163] Neither measure received committee action in the prior Congress.

D. Other Retention Practices

Mandatory retention periods have been adopted for a variety of records. The European Parliament has adopted data retention requirements for electronic records. Many other electronic records are subject to retention standards concerning health, employment and banking records.

1. Data Retention Directive

In 2006, the European Parliament in Brussels adopted a Data Retention Directive requiring up to two years of data retention.[164] The retention period depends on the category of information, including e-

same bill has been introduced in the House by Judiciary Committee Chairman Rep. Lamar Smith and Rep. Debbie Wasserman Schultz").

161. *Id.* § 4.

162. Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act of 2009, S. 436, 111th Cong. § 5 (2009).

163. Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act, H.R. 1076 111th Cong. § 5 (2009).

164. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

mails and phone records. Each member of the European Union must comport their national laws with the Data Retention Directive.

2. Compare Data Retention Requirements for Certain Records

A variety of records, electronic or otherwise, are subject to mandatory retention standards. The retention period for these records ranges from one to ten years. There are numerous medical, banking and employee retention standards at the federal and state levels. Only a few examples are noted below.

Under federal standards, many health care records must be maintained for five years or longer[165] while many states have adopted a ten-year retention period for health care records.[166] Many states also impose a retention requirement for dental records.[167] Certain employment records must be retained for one to five years under federal law.[168] Generally, banking records must be retained for five years under federal law.[169]

165. *See, e.g.*, 42 C.F.R. § 482.24(b)(1) (2011) ("Medical records must be retained in their original or legally reproduced form for a period of at least 5 years."); *id.* § 485.638(c) (medical "records are retained for at least 6 years from date of last entry, and longer if required by State statute, or if the records may be needed in any pending proceeding"). For certain exposure records, a longer period applies. *See* 29 C.F.R. § 1910.1020(d)(1)(ii) (2011) (30-year retention period for records of employees exposed to toxic substances and harmful agents).

166. *See, e.g.*, TENN. COMP. R. & REGS. 1050-02-.18 ("Osteopathic physicians must retain medical records for at least 10 years from the last contact with the patient. However, immunization records and records for incompetent patients must be retained indefinitely and mammography records must be retained for 20 years. X-rays need only be retained for 4 years if there is a document that interprets the image that is kept in the medical record. Medical records of minors must be retained for at least one year after the patient reaches the age of majority or 10 years from the date of last contact, whichever is longer."); 22 TEX. ADMIN. CODE § 165.1(b)(1) ("A licensed physician shall maintain adequate medical records of a patient for a minimum of seven years from the anniversary date of the date of last treatment by the physician."); WASH. REV. CODE § 70.41.190 ("Unless specified otherwise by the department, a hospital shall retain and preserve all medical records which relate directly to the care and treatment of a patient for a period of no less than ten years following the most recent discharge of the patient; except the records of minors, which shall be retained and preserved for a period of no less than three years following attainment of the age of eighteen years, or ten years following such discharge, whichever is longer.").

167. *See, e.g.*, 22 TEX. ADMIN. CODE § 108.8(b) (five-year retention period for dental records); TENN. COMP. R. & REGS. 0460-02-.12 ("All dental records must be retained for at least ten years from the date of the dentist's last contact with the patient.").

168. 29 C.F.R. § 1602.14 (2011) (one year retention period for "personnel or employment record made or kept by an employer" including application forms, and "records having to do with hiring, promotion, demotion, transfer, lay-off or termination, rates of pay or other terms of compensation, and selection for training or apprenticeship").

169. 31 C.F.R. § 103.38 (2010) (five year retention period for covered banking records).

Many of these retention requirements have been in place for decades and many of these records are maintained in electronic form. These records include the most private of information concerning the health, background and financial information of an individual.

The experience with mandatory retention requirements with health, employment, banking and other records is instructive. As with these records, steps can be taken to protect the privacy of the records.

V. Retention Policy Issues

As with other records subject to retention periods, some key policy issues are raised. First, what type of records should be covered? Second, for how long should various records be retained? Is a tiered approach appropriate depending on the records being retained?

A. Types of Records

No suggestion has been made that providers should create new records. The question instead is, given that certain records are created for business purposes and to provide a service to the customer, what types of pre-existing records should be retained?

While there may be other categories, under ECPA, the records generally fall under three categories. The first concerns information about the account holder. This may include the customer's name, address, telephone connection records, or records of session times and durations, length of service, types of service utilized, subscriber identity, and means and source of payment for services rendered.[170] This information may be useful to law enforcement to determine who was using the Internet Protocol address at the time of the crime.

A second category involves non-content information concerning transactional logs.[171] For example, this may identify what Internet Protocol address was connected to the Internet and the activity of the connections, including where and when. The information may reveal data transfers, including volume, and the source and destination of the user. Records could include connection log information.

Finally, a third category would include the content of communications, which may be obtained by a search warrant.[172] Examples would include text or email communications.

170. 18 U.S.C. § 2703(c)(2) (2006).
171. *Id.* § 2703(c)(2)(E).
172. *Id.* § 2703(a).

For law enforcement purposes, the more that can be known about the account, the more helpful it may be in furthering the investigation. For example, Internet Protocol information may show the Internet connections but not the purpose of the connections, which may be revealed by content.

The legislation pending in the House of Representatives falls under the first category, requiring retention for one year of "a log of the temporarily assigned network addresses the provider assigns to a subscriber to or customer of such service that enables the identification of the corresponding customer or subscriber information."[173]

Policy makers can decide what categories of records should be maintained. For example, different health or banking records are retained for different periods.

B. Retention Period

A second question concerns how long the records should be retained. By comparison, some health care records are retained for up to ten years.

Generally, in the criminal justice process, a five-year statute of limitations applies for federal statutes.[174] While there has not been much suggestion for a five-year retention period, the statute of limitations provides an outer limit for policy makers.[175]

The period of retention could be determined by the types of records. This practice has been followed for health, employment, banking and other records. Customer identification and payment records could be subject to a longer retention period than the contents of communications.

173. Protecting Children From Internet Pornographers Act of 2011, H.R. 1981, 112th Cong. § 4 (2011).

174. 18 U.S.C. § 3282 ("Except as otherwise expressly provided by law, no person shall be prosecuted, tried, or punished for any offense, not capital, unless the indictment is found or information is instituted within five years next after such offense shall have been committed."). *See generally* CHARLES DOYLE, CONG. RESEARCH SERV., RL31253, STATUTES OF LIMITATION IN FEDERAL CRIMINAL CASES: AN OVERVIEW (2012), *available at* http://www.fas.org/sgp/crs/misc/RL31253.pdf (contrasting various statutes of limitations for federal offenses).

175. *See generally House Hearings: Data Retention As a Tool for Investigating Internet Crimes*, *supra* note 27, at 68 (statement of Rep. Ben Quayle) (inquiring about matching the retention period with the statute of limitations period).

C. What Access?

A third issue concerns what standard should apply for law enforcement to access the records. This factor becomes relevant because the longer the period of time to obtain the records and the higher the standard, the stronger the justification for a longer retention period.

D. Other Factors

Other factors to consider will include the costs of implementation and other alternatives that may be available.

While storage costs have decreased, the cost will turn in part on the types of records retained. Some have suggested that the retention of some data may not be as costly to maintain.[176] To offset the costs, the House measure disallows a private right of action against any provider for the disclosure of information to law enforcement.[177]

Another issue concerns whether retention may be maintained through other alternatives. For example, some records may be retrievable in backup tapes.[178] Many companies already backup their records in the event they are needed. Some of the requested records may already be included in the scope of backed up records. These and related issues bear on the scope of records that may be retained.

Conclusion

This article has sought to provide a better understanding of the challenges law enforcement confronts in obtaining Internet-based records, often essential to investigate and prosecute crimes involving, at least in part, the Internet. As noted, how much of the trail of Internet evidence will be available often will turn on time and whether the provider has retained them. Because these records are fleeting, law enforcement is normally engaged in a race to obtain them.

As shown, delay is an inherent and inevitable part of the investigative process. In following investigative leads, whether records are present will not be known until legal process is served on the provider.

176. *See, e.g.*, *House Hearings: Making the Internet Safe*, *supra* note 94, at 281 (statement of Michael Angus, Executive Vice President and General Counsel, Fox Interactive Media, MySpace.com) (in responding to the cost "to preserve those IP addresses for 12 months instead of 90 days," noting that "IP logs are such a small amount of data that I can't imagine that it would be cost prohibitive").

177. H.R. 1981, 112th Cong. § 5 (2011).

178. *See, e.g.*, *House Hearings: Making the Internet Safe*, *supra* note 94, at 144 (statement of Dave Baker, Vice President, Law and Public Policy, Earthlink, Inc.) (noting records requested by law enforcement were obtained in backup archives within two weeks).

This process of identifying new leads, preserving the account information, and obtaining and presenting legal process can take many months. Often, after pursuing new Internet leads, law enforcement confronts the "electronic evidence lapse" problem, learning that key records are no longer available.

Case examples also show that without these records, investigations must be closed. This has occurred multiple times concerning sexual exploitation of children offenses.[179]

Before Congress amends ECPA, careful consideration will have to be given to how any proposal will impact law enforcement's ability to investigate and prosecute crime. Any new amendments or standards will impact significant public and criminal justice interests including: (1) undermining confidence in the Internet; (2) hampering the legitimate needs of law enforcement to investigate and solve crimes committed over the Internet; (3) addressing the rights and interests of crime victims; (4) frustrating the specific public policy objectives identified by Congress in enacting a particular criminal statute; (5) in providing a fair process, ensuring that the responsible perpetrators are identified and fairly prosecuted in the criminal justice process; and (6) balancing and respecting privacy interests. Any new proposal to modify the standards should explicitly identify how much delay may result to law enforcement. This will help ensure that the objectives of law enforcement are not undermined.

In any legislative debate, the need to ensure data is retained for law enforcement purposes will be as important today as it was in 1986 when ECPA was first enacted. If new standards are interposed or new delays added, serious consideration should be given to limited retention periods for Internet data. Retention requirements are already used for health, employment, banking and other records between one to ten years. The same privacy concerns that are raised concerning these records, many which are in electronic form, can be adequately protected under ECPA.

In the end, whatever the policy makers decide in amending ECPA, the impact on victims and the ability to attain legislative objectives will turn on the availability of the records.

179. *See supra* Part Intro.C.2.