Northwestern Journal of Technology and Intellectual Property

Volume 11 | Issue 2 Article 2

2013

Public Safety and Online Privacy—Myth Versus Reality

Jason M. Weinstein
Former Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

Public Safety and Online Privacy—Myth Versus Reality

Jason M. Weinstein

January 2013 VOL. 11, NO. 2

Northwestern Journal of Technology and Intellectual Property
Volume 11, Number 2 (January 2013)

Public Safety and Online Privacy—Myth Versus Reality

By Jason M. Weinstein*

¶1 A woman is murdered in her car on a rural road in South Carolina. The county sheriff's office obtains a court order for a suspect's cell phone records on the night of the murder. Cell tower data and calling records enable investigators to determine that the suspect was in the vicinity at the time of the murder, destroying the suspect's alibi and leading him to confess and identify a second person who had arranged the murder. The cell tower data is critical evidence at the trial of that other participant, who is ultimately convicted.

¶2 FBI agents infiltrate a peer-to-peer file sharing network that facilitates the worldwide sharing of child pornography. Agents identify Internet Protocol addresses of members of the network who are producing images of child sexual assault, and subpoenas are used to try to identify the individuals who own those accounts. Building on evidence obtained from the subpoenas, agents develop probable cause for search warrants that result in the identification of seventy-five children who were being sexually abused, most of them under ten years of age.

¶3 Homicide detectives in Louisiana discover a decomposed, burned body. During the investigation that follows, detectives learn that the killer took the victim on a date, brought her back to his apartment, murdered her, and thoroughly cleaned the crime scene. Detectives obtain an arrest warrant for the suspect, only to find that he has fled the state. Using cell tower data obtained by court order, detectives determine the suspect's approximate location and ultimately arrest him.

¶4 The FBI dismantles an international criminal organization that steals victims' identities to raid their bank accounts, causing the victims' banks to transfer huge sums of money from the victims' accounts to accounts controlled by the criminals, resulting in the theft of approximately $30 million over a period of about three years. Using subpoenas and court orders, agents obtain subscriber and call records to help identify and establish connections among members of the organization. Agents later obtain court orders for location information regarding the suspects' cell phones to identify and ultimately arrest them.

¶5 Three individuals use stolen credit card numbers obtained through phishing scams to make more than $3.5 million in fraudulent charges. Early in the investigation, the FBI does not know their identities, their whereabouts, or the full range of their criminal activities. But by using different types of legal process, the FBI is able to obtain information about their communications and build a case against the three targets, who are determined to be in England. Through the ongoing investigation, the FBI learns that the three men are using the proceeds of their identity theft scheme to finance terrorism by hosting jihadi Web sites and purchasing equipment, prepaid cell phones, airline tickets,

* Former Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice

and other items to support jihadi groups in the field. English courts later convict all three, both for their terrorist activities and for their financial crimes.

¶6 These are not hypotheticals – they are all real cases. And, all of these cases were successfully investigated and prosecuted only because law enforcement agents and prosecutors were able to obtain, through lawful process, location information and other data relating to electronic communications.

¶7 The explosive growth of the Internet and other modern forms of communication has revolutionized nearly every aspect of our lives, but it has also revolutionized crime and national security threats. From around the corner or around the globe, skilled hackers and criminal organizations work every day to access the computer systems of government agencies, universities, banks, merchants, and credit card companies to steal large volumes of personal information and to perpetrate large-scale data breaches that leave tens of millions of Americans at risk of identity theft.[1] Our computers and networks are also increasingly at risk from criminals who seek to infect them with malicious code to make them part of a botnet: a network of compromised computers under the remote command and control of cybercriminals who can capture every keystroke, mouse click, password, credit card number, and e-mail.

¶8 Over the last decade, we have also witnessed an explosion of mobile computing technology. From laptops and cell phones to tablets and smartphones, Americans are using mobile computing devices more extensively than ever before.[2] We can bank, shop, conduct business, and socialize remotely with our friends and loved ones instantly, almost anywhere. Now more than ever, the world is almost literally at our fingertips. But as the use of mobile devices continues to grow, these devices are becoming increasingly tempting targets for identity thieves and other criminals.

¶9 Consequently, as our mobile devices increase our connectivity, productivity, and efficiency, they also pose potential threats to our safety and privacy. Smartphones and tablets are, in a very real sense, mobile computers. As the line between mobile devices and personal computers continues to shrink, these devices provide yet another computing platform for cybercriminals to target for botnets and infection by malicious code. Unfortunately, Americans using infected computers and mobile devices suffer from an ongoing, pervasive invasion of their privacy at the hands of these criminals almost every time they turn on their devices.[3]

---

[1] *See, e.g.*, Grant Gross, *Two Romanians plead guilty in Subway hack,* COMPUTERWORLD (Sept. 17, 2012, 5:37 PM), http://www.computerworld.com/s/article/9231373/Two_Romanians_plead_guilty_in_Subway_hack?taxonomyId=85; Jason Schreier, *Sony Hacked Again; 25 Million Entertainment Users' Info at Risk*, WIRED (May 2, 2011, 7:11 PM), http://www.wired.com/gamelife/2011/05/sony-online-entertainment-hack/.

[2] *See, e.g.*, Aaron Smith, *Cell Internet Use 2012*, PEW INTERNET & AMERICAN LIFE PROJECT (June 26, 2012), http://pewinternet.org/Reports/2012/Cell-Internet-Use-2012.aspx. The Pew Research Center reports that, as of April 2012, approximately 88% of American adults use a cell phone and more than half use their phone to go online. The report notes that this saturation marks a notable growth from the 31% of cell phone owners who said they used their phones to go online as of April 2009.

[3] For example, in April 2011, the Department of Justice took judicially-authorized action to disrupt and ultimately disable the "Coreflood" botnet, which was recording and "stealing private personal and financial information from unsuspecting computer users" across the United States. Press Release, United States Attorney's Office Dist. of Conn., Department of Justice takes Action to Disable International Botnet (April 13, 2011), http://www.justice.gov/usao/ct/Press2011/20110413-1.html.

¶10 But identity theft is far from the only type of crime committed using online means. On the contrary, the Internet and modern communication technologies are used to facilitate virtually every type of crime imaginable. Because criminals of all types use cell phones, mobile devices, and Internet-based means of communication more than ever, electronic evidence is now critical in prosecuting cases involving terrorism, espionage, violent crime, drug trafficking, kidnapping, computer hacking, sexual exploitation of children, organized crime, gangs, and white collar offenses. Without evidence from the online world, it is becoming increasingly difficult, if not impossible, to investigate and prosecute all types of "real world" crimes.[4]

¶11 Simply put, electronic evidence has never been more important to the protection of public safety. At the same time, concern is growing among Internet users about their privacy in the online world, and the nation is now engaged in a robust and important discussion about how best to balance privacy with public safety and business growth and innovation.

¶12 The Electronic Communications Privacy Act (ECPA), enacted in 1986 and amended several times since in an effort to keep up with changing technology, establishes the rules of the road for law enforcement access to stored electronic communications data, striking a balance between public safety needs and privacy.[5] Congress is now considering whether the ECPA continues to strike that balance properly.[6] And now, with the decision in *United States v. Jones* regarding the use by law enforcement of GPS trackers on cars,[7] the Supreme Court has put its own stamp on this national discussion.

¶13 All Internet users—from individual consumers to businesses both large and small—have a significant interest in the outcome of this debate. And all stakeholders—law enforcement agencies, consumers, privacy groups, and businesses alike—have important perspectives that must be weighed carefully and thoughtfully. Unfortunately, as part of this debate, rhetoric about law enforcement's ability to access online information often bears little resemblance to reality. In the interests of promoting a more informed discussion of these issues, this article debunks three common myths about law enforcement and online privacy.

Myth #1: Law enforcement officials can obtain whatever location information or other electronic evidence they want, whenever they want it.

¶14 The reality is that in order to compel providers to disclose location information or other electronic evidence, law enforcement officers are required to use lawful process. The type of process that is required and the level of evidentiary threshold that must be satisfied depend on the nature of the information that law enforcement officers seek to obtain.

---

[4] *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. on Privacy, Tech. and the Law of the S. Judiciary Comm.*, 112th Cong. (2011) *available at* http://www.judiciary.senate.gov/pdf/11-5-10%20Weinstein%20Testimony.pdf (statement of Jason Weinstein, Deputy Assistant Att'y Gen.).

[5] Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848,(1986) (codified as amended in scattered sections of 18 U.S.C. (2006)).

[6] Juliana Gruenwald, *Senate Judiciary to Take Up Privacy Legislation*, NATIONAL JOURNAL (Sept. 11, 2012, 2:00 PM), http://techdailydose.nationaljournal.com/2012/09/senate-judiciary-to-take-up-pr.php.

[7] *See United States v. Jones*, 132 S. Ct. 945 (2012).

¶15 To require the production of certain types of information, such as precise location information from a cell phone or real-time interception of the contents of e-mails, law enforcement officials must first obtain a search warrant or court order based on a showing of probable cause.[8] For other types of information, such as to/from "header" information for e-mails or historical records regarding what cell towers were used to connect cell phone calls, law enforcement officers must first secure a court order based on a showing of "specific and articulable facts" demonstrating that there are reasonable grounds to believe that the information is relevant and material to a criminal investigation.[9] For a subset of information specified by statute, often referred to as basic subscriber records, a subpoena is required.[10]

¶16 Some have criticized the ECPA as permitting "warrantless" access by law enforcement to certain types of information, suggesting that a warrant based on a showing of probable cause should be required for all types of electronic evidence.[11] But "warrantless" does not mean that law enforcement has a blank check—quite the opposite. Even in those situations where a search warrant is not required, some other type of process—often including judicial review and findings supporting a court order—is required.[12] Our laws regarding access to electronic evidence reflect a recognition that law enforcement officers typically do not begin an investigation already having probable cause for warrants or wiretaps. On the contrary, agents and prosecutors must use other less intrusive techniques as "building blocks" to develop probable cause. For example, investigators use telephone calling records or general information about the approximate location of cell phones at the early stage of investigations to identify members of a conspiracy, establish possible connections between individuals, and build probable cause to obtain wiretap orders, search warrants, and arrest warrants. Just as often, that kind of "building block" information is used to *exclude* people as suspects, which helps prevent additional intrusions into the lives of innocent people, allowing police to focus on the proper targets. If prosecutors did not have the ability to use legal process short of a warrant to build cases, the ability of law enforcement to protect public safety and privacy would be seriously compromised because many crimes would go unsolved and many criminals—from identity thieves to child predators to murderers—would go unprosecuted.

---

[8] *See* 18 U.S.C. §§ 2516, 2518, 2703(c)(1)(A) (Supp. 2011).

[9] *See* 18 U.S.C. § 2703(c)(1), (d) (Supp. V 2011).

[10] 18 U.S.C. § 2703(c)(2) (Supp. V 2011).

[11] *See, e.g.*, Mark Jaycox & Lee Tien, *ECPA Reform May Require Warrants for Email, But Hurts Video Privacy*, ELECTRONIC FRONTIER FOUNDATION (Sept. 19, 2012), https://www.eff.org/deeplinks/2012/09/ecpa-reform-may-require-warrants-email-hurt-video-privacy; *ECPA Reform: Why Now?*, DIGITAL DUE PROCESS, http://www.digitaldueprocess.org/index.cfm?objectid=FE5C92F0-2552-11DF-B455000C296BA163 (last visited Oct. 15, 2012).

[12] *See* 18 U.S.C. § 2703(d) (Supp. V 2011).

Myth #2: Law enforcement can use cell phones to track users without first obtaining a court order.

¶17 The reality is that to compel a phone company to provide any location information about a criminal suspect's cell phone, law enforcement must obtain a court order based on a significant evidentiary showing.

¶18 As a general matter, cell phone location information can be divided into two broad categories: cell tower information and precision-location information, often referred to as "GPS." In order to require a cell phone company to disclose precision-location information for a suspect's cell phone, law enforcement obtains a warrant based on a showing of probable cause. This may come as a surprise to some, given depictions on television, but it is a fact.

¶19 Cell tower information consists of the records made by a cellular network provider indicating which cell tower serves a user's phone when that user places or receives a call or text message. Those records are generated only while the cell phone is being used during a call or text message and not while the phone is idle. Cellular providers create and maintain these records in the ordinary course of business to facilitate providing wireless service to their customers. Cell tower records do not reveal the precise location of a user's cell phone. They reveal only the physical location of the cellular antenna serving a user's phone and, by extension, the effective service area of that antenna. The service area will vary depending on factors such as terrain, signal strength, and cell tower density. Moreover, depending on call volume, the cell tower serving a user's phone may not even be the tower closest to that phone.

¶20 Law enforcement officers must seek authorization from a court to obtain cell tower records for a suspect's cell phone, even if those records are for calls made in the distant past. For historical records, courts require law enforcement to obtain a court order based on a showing of "specific and articulable facts" demonstrating that the information is relevant and material to a criminal investigation. To obtain such records prospectively, some courts require an order based on a showing of "specific and articulable facts," while other courts require a warrant based on probable cause.[13] While "specific and articulable facts" is a lower standard than probable cause, it is certainly not a low standard. On the contrary, it provides a substantial degree of privacy protection and robust judicial review, and it was hailed as such by some privacy groups when Congress imposed that standard in 1994.[14]

¶21 It is also worth noting that, under existing law, location information regarding a suspect's cell phone is already far more protected than many other types of information about the suspect's location. Indeed, if a suspect makes a landline call from his home phone, a record of that call can establish that, at a particular time, the suspect was in his home—perhaps the most private space protected by the Constitution. Yet, such records can be obtained by grand jury subpoena on a far lower showing than "probable cause" or even "specific and articulable facts."

[13] *See* 18 U.S.C. § 2703(d) (Supp. V 2011) (historical); 18 U.S.C. §§ 2703(d), 3122-24 (Supp. V 2011) (prospective).

[14] *See, e.g.*, *EFF Statement on and Analysis of Digital Telephony Act*, ELECTRONIC FRONTIER FOUND. (Oct. 8, 1994), https://w2.eff.org/Privacy/Surveillance/CALEA/digtel94_passage_statement.eff.

¶22 Moreover, by living "on the grid," a suspect necessarily leaves a trail of evidence regarding his movements and location. For instance, suppose that in the course of a day a suspect makes a landline call from his home phone, uses an ATM machine, parks in a parking garage equipped with a security camera, goes to Starbucks and pays with a credit or debit card, and sends money from a Western Union store. Records of those transactions would provide a picture of the suspect's movements over the course of the day, and all of those records—from receipts and other documents to security camera footage—could be obtained by law enforcement with a grand jury subpoena, which requires only that the information sought be relevant to a criminal investigation. Similarly, pursuant to subpoena, law enforcement can obtain testimony from eyewitnesses as to a suspect's precise location at a particular time. Yet law enforcement must apply to a court for an order based on a showing of "specific and articulable facts" in order to learn the location of a cell tower that reveals only the general vicinity of a suspect's cell phone during a call that occurred months earlier. Simply put, cell phone location information already enjoys a higher level of protection from law enforcement access than other types of information that reveal a suspect's location.

Myth #3: There is a conflict between law enforcement's efforts to protect public safety and the privacy of individuals.

¶23 The reality is that "public safety vs. privacy" is a false dichotomy. One of the Justice Department's core missions is protecting Americans' privacy by investigating and prosecuting the hackers, identity thieves, cyberstalkers, and other criminals who threaten that privacy. It actually harms Americans' privacy if hackers, identity thieves, and other criminals are able to access personal information while law enforcement is prohibited from obtaining the data it needs to catch them. Truly protecting privacy requires not only that individuals protect their personal information from criminals who seek to steal it, but also that law enforcement is able to use the evidentiary building blocks necessary to capture and prosecute those who violate the laws that protect an individual's privacy.

¶24 To put this debate into perspective, it is worth noting that law enforcement requests made to online providers for information about Internet activity affect only a relatively small number of online users. For example, during 2011, law enforcement agencies in the United States—local, state, and federal combined—requested data relating to specific accounts for approximately 23,300 Google users, representing only approximately .0058% of all registered Google users.[15] By contrast, 100% of Internet users are at risk from identity thieves and other criminals who threaten their privacy every time they turn on their computers. While law enforcement makes a much larger number of requests for

[15] *Transparency Report*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/?p=2011-06 (last visited Oct. 16, 2012) (Jan.–June 2011); *Transparency Report*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/?p=2011-12 (last visited Oct. 16, 2012) (July–Dec. 2011). Google reports having over 400 million registered users. If one were to use Google's estimate of approximately one billion unique users, the percentage of affected users drops to approximately .0023%. *See* Emily Protalinski, *As predicted, Google+ passes 400M registered users, now has 100M monthly active users*, THE NEXT WEB (Sept. 17, 2012) http://thenextweb.com/google/2012/09/17/as-predicted-google-passes-400m-registered-users-now-100m-monthly-active-users/. I conservatively approximated one billion unique Google users. *See also Google's New Record, 1 billion visitors in May*, IT'S ALL TECH, http://itsalltech.com/2011/06/22/googles-new-record-1-billion-visitors-in-May (June 22, 2011, 12:16 PM).

information from cell phone providers for information about cell phone activity, the volume of such requests simply reflects the rise in the use of cell phones by criminals to facilitate their crimes, making information about suspects' cell phone use an increasingly important tool in criminal investigations. Moreover, when federal law enforcement seeks access to electronic communications, location information, or other online or cell phone records, it does so under rules set forth by statute, with judicial oversight, for the sole purpose of *solving crimes* and *catching criminals*.

¶25 So, in considering whether to rewrite the standards that govern law enforcement access to electronic data, policy makers need to consider that choices made out of a desire to enhance privacy may ultimately reduce it, by making it difficult—and in some cases impossible—for law enforcement to pursue the criminals who pose a threat to privacy. More broadly, those choices will have very real consequences for public safety, as they will significantly reduce the ability of law enforcement to investigate and prosecute a wide array of serious crimes.

Conclusion

¶26 The national discussion about technology, public safety, and privacy is critically important for all Americans. But if that discussion is to advance the goal of protecting public safety and privacy while also fostering innovation and economic growth, it must be guided by reality, not myth. The reality is that dedicated federal agents and prosecutors throughout the country are committed to protecting public safety and catching and deterring criminals who threaten privacy by stealing identities and other private information. They go about this important work while respecting the privacy of citizens, by complying with all applicable legal standards and obtaining appropriate legal process, with appropriate judicial review, at every stage of every investigation. If those legal standards are raised in a way that effectively puts critical evidence out of the reach of law enforcement, public safety will suffer, and privacy will suffer along with it.

Northwestern Journal of Technology and Intellectual Property

Volume 11, Number 2 (January 2013)