The Law Enforcement Surveillance Reporting Gap

Christopher Soghoian[♦]

[Draft Version 1.1: Please send feedback to chris@soghoian.net]

> "[T]here are known knowns; there are things we know we know.
> We also know there are known unknowns; that is to say we know there are some things we do not know."
>
> Donald Rumsfeld, United States Secretary of Defense, February 12, 2002.

Section I: Introduction

Wiretaps, at least In Hollywood, often involve FBI agents hiding in an unmarked van outside a suspect's home, crouched over a set of headphones, as they listen to telephone calls taking place inside.[1] Similarly, the seizure of digital evidence often involves a pre-dawn raid by a team of armed agents, who

♦ Graduate Fellow, Center for Applied Cybersecurity Research, PhD Candidate, School of Informatics and Computing, Indiana University. Email: chris@soghoian.net. Other research papers available at http://www.dubfire.net. Thanks to Kevin Bankston, Fred Cate, Catherine Crump, Al Gidari, Paul Ohm, Julian Sanchez and Paul Schwartz.

© 2011 Christopher Soghoian. The author hereby permits the use of this article under the terms of the Creative Commons Attribution 3.0 United States license, the full terms of which are available at http://creativecommons.org/licenses/by/3.0/us/legalcode.

[1] Whitfield Diffie & Susan Landau, *Communications surveillance: Privacy and Security at Risk*, 52 COMMUNICATIONS OF THE ACM 42 (2009), (last visited Mar 6, 2011)("We all know the scene: It is the basement of an apartment building and the lights are dim. The man is wearing a trench coat and a fedora pulled down low to hide his face. Between the hat and the coat we see headphones, and he appears to be listening intently to the output of a set of alligator clips attached to a phone line. He is a detective eavesdropping on a suspect's phone calls. This is wiretapping—as it was in the film noir era of 1930s Hollywood. It doesn't have much to do with modern electronic eavesdropping, which is about bits, packets, switches, and routers.")

Electronic copy available at: http://ssrn.com/abstract=1806628

later emerge from the target's home with computers, documents and various types of storage media. In the movies, law enforcement agents obtain the evidence themselves, usually at great personal risk. [2]

While these investigative methods look great on the big screen, they are largely a relic of the past – from an era before modern telecommunications providers, cloud computing and mobile phones. These days, the police or FBI can obtain most of the data they need from the comfort and safety of their own desks, with a few clicks of a mouse, a fax, or a phone call to a telecommunications or Internet service provider.[3] The actual collection of evidence is now increasingly performed by the same companies that consumers rely on to transmit and store their phone calls, emails and documents.

Consider the following sources of information that are used in modern law enforcement investigations: Wiretaps and electronic communications intercepts, stored emails, instant messages, web browsing history and search engine records, as well as geo-location information from mobile phones, both historical and real-time. All of these are delivered to the government by third party service providers. Law enforcement agents play little to no role in actually acquiring the data. They simply submit the name or phone number of a suspect and then wait for the company to deliver its customers' private files.

Third party facilitated surveillance has become a routine tool for law enforcement agencies. [4] There are likely hundreds of thousands of such requests per year. Unfortunately there are few detailed statistics documenting the use of many modern surveillance methods. As such, the true scale of law enforcement surveillance, although widespread, remains largely shielded from public view.

Prior to the widespread adoption of the Internet and mobile phones, law enforcement agencies' use of third party facilitated electronic surveillance was largely limited to real-time interception of communications content ("wiretapping") and non-content data (through the use of "pen register" and "trap and trace" orders). In order to increase its ability to perform effective oversight, Congress

[2] IN SOFTLEY, HACKERS (MGM (Video & DVD)) (1998)

[3] *US v. Pineda-Moreno*, 617 F. 3d 1120 - Court of Appeals, 9th Circuit 2010. Dissent by Kozinski at 1126 ("When requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that 'such dragnet-type law enforcement practices" are already in use.'")

[4] *See*, e.g., Saul Hansel, *Online Trail Can Lead to Court*, N.Y. TIMES, Feb. 4, 2006, at C6 ("Who is sending threatening e-mail to a teenager? Who is saying disparaging things about a company on an Internet message board? Who is communicating online with a suspected drug dealer? These questions, and many more like them, are asked every day of the companies that provide Internet service and run Web sites. **And even though these companies promise to protect the privacy of their users, they routinely hand over the most intimate information in response to legal demands from criminal investigators and lawyers fighting civil cases... Requests for information have become so common that most big Internet companies, as well as telephone companies, have a formal process for what is often called subpoena management.** Most of the information sought about users is basic, but very personal: their names, where they live, when they were last online—and, if a court issues a search warrant, what they are writing and reading in their e-mail."). (emphasis added)

Electronic copy available at: http://ssrn.com/abstract=1806628

mandated that annual reports be created documenting the use of these surveillance powers. These reports are intended to enable policy makers as well as the general public to determine the extent to which such surveillance methods are used, and in the words of Senator Patrick Leahy, provide a "far more reliable basis than anecdotal evidence on which to assess law enforcement needs and make sensible policy in this area."[5]

The existing surveillance statistics might be sufficient if law enforcement agencies' surveillance activities were limited to wiretaps and pen registers. However, over the last decade, law enforcement agencies have enthusiastically embraced many new sources of investigative and surveillance data for which there are no mandatory reporting requirements. As a result, most modern surveillance now takes place entirely off the books and the true scale of such activities, which vastly outnumber traditional wiretaps and pen registers, remains unknown.[6]

This article will proceed as follows. Section II examines the existing electronic surveillance reporting requirements and the reports that have been created as a result. Some of these have been released to public, but many have only come to light as a result of Freedom of Information Act requests or leaks by government insiders. Section III examines several law enforcement surveillance methods for which there are no existing legally mandated surveillance reports. Finally, section IV proposes specific legislative reporting requirements in order to enable some reasonable degree of oversight and transparency over all forms of law enforcement electronic surveillance.

[5] 145 Cong. Rec. 31,311 (1999) (statement of Sen. Leahy).

[6] According to a letter sent by a Verizon executive to members of Congress in 2007, the company receives approximately 90,000 requests from law enforcement agencies each year. See: Randal S. Milch, Sr. Vice Pres., Verizon Bus., to John D. Dingell, Edward J. Markey & Bart Stupak, U.S. Reps (Oct. 12, 2007), available at http://markey.house.gov/docs/telecomm/Verizon_wiretaping_response_101207.pdf. Contrast this to the approximately 12,500 pen register and 11,000 trap and trace orders obtained in 2009 by agencies within the Department of Justice (see: http://files.spyingstats.com/pr-tt/doj-high-level-pr-tt-2009.pdf) and the approximately 2300 wiretap orders issued nationwide in 2009 (See: http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2009/Table2.pdf).

Table of Contents

Section II: Surveillance methods for which there are official reports

Although law enforcement agencies have many electronic surveillance powers, official reports only exist for a few types, primarily those that relate to the real-time interception of data. This section will explore each of these law enforcement surveillance powers and examine specific trends detailed in the reports.

Electronic intercepts ("wiretaps")

In 1968, after a series of high-profile Supreme Court decisions,[7] Congress established federal rules governing the use of real-time electronic intercepts ("wiretaps").[8] This law, the Omnibus Crime Control and Safe Streets Act, also required the Administrative Office of the US Courts to compile and submit to Congress detailed annual reports on the use of wiretaps and other forms of electronic surveillance by law enforcement agencies.[9] The legislative history states that:

> [The wiretap reports] are intended to form the basis for a public evaluation of its operation. The reports are not intended to include confidential material. They should be statistical in character… [they] will assure the community that the system of court-order electronic surveillance envisioned by the proposed chapter is properly administered and will provide a basis for evaluating its operation. [10]

---

[7] *See* generally*: Berger v. New York*, 388 U.S. 41 (1967) and *Katz v. United States*, 389 U.S. 347 (1967).

[8] Surveillance statistics played an important role in the passage of this first wiretapping law. Supporters of enhanced law enforcement powers argued that existing state wiretapping authority was neither widely used nor abused. For example, the legislative history notes that:

> When the facts are brought to light, statistics show that extremely few telephones are tapped by law enforcement officers -- and that even fewer electronic surveillance devices are installed…In its report the [New York State legislative] committee explicitly declared that no abuses whatever by any district attorney had been found in the use of the wiretapping privilege… Law enforcement officers simply have too much to do to be listening in on conversations of law-abiding citizens. Available manpower just does not permit such abuse. It is idle to contend otherwise. (see: S. REP. 90-1097, S. Rep. No. 1097, 90TH Cong., 2ND Sess. 1968, 1968 U.S.C.C.A.N. 2112, 1968 WL 4956 (Leg.Hist.))

[9] These other forms of electronic surveillance include hidden microphones ("bugs"). As such surveillance is performed directly by law enforcement agencies without the assistance of third parties, they are beyond the scope of this article.

[10] S. REP. 90-1097, S. Rep. No. 1097, 90TH Cong., 2ND Sess. 1968, 1968 U.S.C.C.A.N. 2112, 1968 WL 4956 (Leg.Hist.)

The reports are extremely detailed, and for each wiretap, reveals the city or county, the kind of interception (phone, computer, pager, fax), the number of individuals whose communications were intercepted, the number of intercepted messages, the number of arrests and convictions that resulted from the interception, as well as the financial cost of the wiretap.[11]

By all indications, the Administrative Office of the US Courts has done a good job in making sure that the reports are accurate and submitted to Congress in a timely manner, and has even drawn praise from Congress for doing so. [12] Since at least 1998, the Administrative Office has also made copies of these reports available to the general public via its website.[13] As such, the release of the annual report usually leads to media coverage regarding the increased use of wiretaps.[14]

Analysis of existing reports

The Administrative Office of the Courts has published reports for the years 1997 to the present.[15] By comparing these reports, several interesting trends can be seen regarding the use of this surveillance power by federal and state law enforcement agencies.

Wiretap requests are increasing, but rarely rejected by the courts

Between 1987 and 2009, law enforcement agencies requested over 30,000 wiretap orders. Requests have increased each year: In 1987, there were 637 wiretap orders requested nationwide; ten years later, the number increased to 1186; in 2009, the most recent year for which reports exist, 2376 wiretaps were requested.

---

[11] 18 U.S.C. § 2519(2)–(3) (2006) (outlining what the intercepted communications report issued by the Administrative Office of the United States Courts must contain).

[12] 145 Cong. Rec. 31,311 (1999) (statement of Sen. Leahy) ("The AO has done an excellent job of preparing the wiretap reports.").

[13] http://web.archive.org/web/19981206135425/www.uscourts.gov/wiretap/contents.html

[14] *National News Briefs; Record Total of Wiretaps Was Approved by Courts*, THE NEW YORK TIMES, May. 10, 1998, http://www.nytimes.com/1998/05/10/us/national-news-briefs-record-total-of-wiretaps-was-approved-by-courts.html (last visited Apr 3, 2011); Susan Stellin, *Compressed Data; Who's Watching? No, Who's Listening In?*, THE NEW YORK TIMES, Jun. 3, 2002, http://www.nytimes.com/2002/06/03/business/compressed-data-who-s-watching-no-who-s-listening-in.html (last visited Apr 3, 2011); http://www.wired.com/threatlevel/2010/04/wiretapping/,

[15] See: http://www.uscourts.gov/Statistics/WiretapReports.aspx

During the more than 20 years for which public data exists, requests for wiretap orders have been rejected just 7 times, twice in 1998, once in 1996, twice in 1998, once in 2002 and once in 2005. Similarly, during the last decade, courts required that 580 requests be modified before granting them.[16]

The low number of rejections is not particularly encouraging, and seems to suggest that the courts are essentially "rubber stamping" wiretap orders. Similarly, the 2nd Circuit Court of Appeals recently cited the almost 100% approval rate of the Foreign Intelligence Surveillance Court (FISC) in suggesting that there is insufficient oversight of such surveillance.[17] On the other hand, a number of former federal prosecutors that I've spoken to claim that the high approval rates for wiretap and FISA surveillance likely reflect the vigorous internal quality controls within the Department of Justice.[18] Assuming that this theory is correct (something I cannot independently verify), it is unclear if similar controls exist within state attorneys general, even though state courts also rarely reject wiretap applications.

Wiretaps primarily target mobile phones

Over the past decade, the number of wiretaps involving fixed locations (such as homes or businesses) has declined in favor of intercepts of mobile phones. For example, 96 percent (2,276 wiretaps) of all authorized wiretap for 2009 are for portable devices.[19] As described earlier, the number of wiretaps has

[16] Between 1997 and 2001, courts modified 8 intercept orders each year before granting them. In 2002, that number increased to 94, and has stayed above 45 in all of the years that followed. It is unclear what happened in 2002 that resulted in this exponential increase in modified requests.

[17] *Amnesty International USA v. Clapper*, http://www.aclu.org/files/assets/09-4112_opn.pdf at page 42. ("The [FISA Amendments Act] does not require or even permit the FISC to make an independent determination of the necessity or justification for the surveillance… Empirical evidence supports this expectation: In 2008, the government sought 2,082 surveillance orders, and the FISC approved 2,081 of them. We do not know how many of these applications, if any, came after the FAA was enacted on July 10, 2008.")

[18] Email from Professor Paul Ohm to Christopher Soghoian, April 8, 2011, on file with author ("Yes. I can't vouch for what happens at the state level (except to note that in many states, wiretaps are rarely used), but at the federal level, all proposed wiretap orders must be approved by the Office of Enforcement Operations (OEO) at Main Justice before they can be submitted to a court. In my experience, line attorneys in the field consider the OEO to be a significant hurdle, because they have learned that OEO will return any proposed wiretapping order that fails to scrupulously live up to Title III's standards. I believe it is routine to need to return to OEO with several successive drafts of a proposed order, with each draft bearing a narrower scope than the one before."); another former federal prosecutor echoed the same point, but would not go on the record.

[19] See http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2009/2009Wiretaptext.pdf

gone up each year over the past few decades. However, the statistics suggest that this increase is entirely due to increases in the number of mobile devices monitored.[20]

There are several factors that may explain this trend. First, our society has increasingly "cut the cord" and embraced mobile phones.[21] It is understandable that law enforcement agencies have followed their targets to this new technology. This trend is even stronger among young people and the poor, both of whom are generally more likely to be subject to investigation by the government. Second, it is far easier to wiretap mobile devices. Such intercepts can be performed from the comfort of a desk, rather than requiring that a phone company employee visit a remote office or exchange in order to intercept the line. The reason for this difference is that a majority of traditional wire-line telephone switches do not support modern interception technologies, in contrast to wireless switches, all of which support such interception capabilities.[22]

Roving authority is rarely used

Law enforcement agencies can obtain special "roving" intercept orders if they can demonstrate probable cause to believe that the target is actively thwarting interception at a specific location,[23] such as by using and abandoning low-cost mobile phones ("burners").[24] Although government officials often

[20] In 1997, the first year that reports are available on the web, there were 382 residential wiretaps, 78 at places of business, 185 combination orders (for multiple locations), and 529 "other" (which presumably included early mobile devices). By 2001, the administrative office of the courts created a new separate category to track mobile devices. By that time, there were just 206 residential wiretaps, 60 at places of business, 117 combination orders, and just 83 "other". There were however, 1007 portable devices monitored that year. Nearly a decade later, in 2009, there were just 19 residential, 10 at places of business, 55 combination orders and 13 "other."

[21] Pew Internet and American Life Project, *A Closer Look at generations and cell phone ownership*, February 3, 2011, *available at* http://www.pewinternet.org/Infographics/2011/Generations-and-cell-phones.aspx ("85% of Americans age 18 or older own a cellphone, making it by far the most popular device among adults.)

[22] Ryan Singel, *DCS-3000 is the FBI's New Carnivore*, Posting to Threat Level Blog, available at http://www.wired.com/threatlevel/2006/04/dcs3000_is_the_/ (Apr. 17, 2006, 19:04) ("[S]ome 80 to 90 percent of old-fashioned wireline phone switches are apparently not CALEA compliant, which means the feds still have to perform those taps the old fashioned way. But every wireless switch in the country is CALEA ready . … [and] [o]ver 80 percent of intercepts are now targeting wireless phones…").

[23] 18 U.S.C. § 2518(11)(a) and (b).

[24] The Wire Episode 4, season 3 at 00:42:23 ("They make a couple of calls with a burner, throw it away. Go on to the next phone, do the same. There's more of those things laying around the streets of West Baltimore than empty vials." "Well, how the fuck you supposed to get a wire up on that?" "Yeah, well, first it was payphone and pagers. Then it was cell phones and face-to-face meets. Now this. The motherfuckers do learn. Every time we come at them, they learn and adjust."); Jim Dwyer, *It's Not Just Drug Dealers Who Buy Prepaid Phones*, THE NEW YORK TIMES, May. 28, 2010, https://www.nytimes.com/2010/05/30/nyregion/30about.html (last visited Apr

cite the use of disposable phones by drug dealers,[25] the wiretap reports reveal that roving orders are rarely sought. Over the past thirteen years, just over 13 roving orders on average have been issued nationwide each year, with a high of 27 orders issued in 2000, and a low of 1 order issued in 2004.

Surveillance and the war on drugs

The reports reveal one of the lesser known side effects of the war on drugs: the expansion of the surveillance state. The latest report reveals that more than 86 percent of the 2306 wiretap orders obtained by federal and state law enforcement agencies were sought in narcotics investigations.[26] The next largest categories are homicide/assault, "other" and racketeering, which were each specified in 4 percent, 3 percent and 3 percent, respectively, of applications. Earlier reports over the last decade confirm similar percentages.

These numbers are not too surprising, given that the earliest wiretapping cases involved government efforts to investigate bootleggers.[27] While the particular drug has changed, law enforcement surveillance resources still seem almost entirely dedicated to enforcing prohibitions.

5, 2011)("Last fall, during a narcotics raid on an apartment in Astoria, the authorities found 22 prepaid cellphones, and plenty of cash to pay for them: $133,000. Among the names people in New York City have used when buying prepaid cellphones are Lady Gaga, King Kong, Sugar Love and Jesus Mom, according to investigators with the Office of the Special Narcotics Prosecutor.")

[25] Speech by President George W. Bush, Buffalo, NY, April 20, 2004 available at http://rawstory.com/news/2005/Bush_claimed_taps_required_warrants_in_1220.html ("But a roving wiretap means-it was primarily used for drug lords. A guy, a pretty intelligence [sic] drug lord would have a phone, and in old days they could just get a tap on that phone. So guess what he'd do? He'd get him another phone, particularly with the advent of the cell phones. And so he'd start changing cell phones, which made it hard for our DEA types to listen, to run down these guys polluting our streets. And that changed, the law changed on-roving wiretaps were available for chasing down drug lords.");

[26] See: http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2009/Table3.pdf

[27] *Olmstead v. United States*, 48 S.Ct. 564, 277 U.S. 438 (1928).

Wiretaps of computers and email

The wiretap reports include specific categories describing the location and type of intercept order. One such category is "computer or email (electronic)," which refers to those orders used to intercept data in transit to a computer. The reports reveal that since 1997, federal law enforcement agencies have obtained just 67 such intercept orders and 54 have been issued to the state law enforcement agencies.

Based upon these numbers, it seems pretty clear that law enforcement agencies rarely engage in real-time interception of Internet communications, even as they continue to increase their use of mobile telephone surveillance. At first blush, this seems rather counterintuitive, given the degree to which our society has become dependent upon email, instant messages, social networks and other Internet based communications. However, there are many ways for law enforcement agencies to monitor internet communications,[28] and it is often easier and cheaper to do it after the fact rather than in real-time.[29] As I will explain later in this article, there are no official statistics regarding law enforcement acquisition of stored communications data.

Incidents of cryptography encountered in criminal investigations

During the late 90s, senior law enforcement officials repeatedly complained to Congress that they were "going dark" and losing the ability to intercept communications as criminals embraced encryption technologies.[30] Responding to these claims and a report from the U.S. Working Group on Organized Crime,[31] Congress amended the existing wiretap reporting statute in 2000 to include statistics on the number of intercept orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications.[32] These encryption reports, Senator Leahy argued at the time, would be "a far more reliable basis than anecdotal evidence on which to assess law enforcement needs and make sensible policy in this area."

---

[28] This is because network communications are often retained for long periods of time. For example, if the police do not wiretap a telephone call, they will not be able to access it content at a later date. However, if the police do not intercept an email as it is sent over the network, they can always go to the suspect's email provider days or weeks later to obtain a copy of it.

[29] Regarding ease: Intercepting an email "in transit" requires a super-warrant, but at most a probable cause warrant once it has been received by the user's ISP. With regard to cost: As an example, consider that Cox Communications charges $2,500 for a pen register and $3,500 for a wiretap, whereas account information only costs $40.00. see: http://ww2.cox.com/aboutus/policies/lea-information.cox

[30] Statement of Louis J. Freeh, Director, Federal Bureau of Investigation, Before the, Senate Judiciary Committee, July 9, 1997, *available at* http://epic.org/crypto/legislation/freeh_797.html, ("The looming spectre of the

According to these reports, during the last decade, there have been a total of 91 instances in which encryption was encountered during a federal or state wiretap, and not a single instance in which the encryption prevented law enforcement officials from obtaining the plain text of communications intercepted. Furthermore, over the past 4 years, the number of instances in which encryption was encountered has plunged to less than 2 cases per year. [33] These numbers strongly contradict the earlier claims by law enforcement officials regarding the impact of encryption technology.[34]

Year	State and federal wiretaps in which encryption was encountered	Wiretaps where encryption prevented officials obtaining plain text of communications
2000	22	0
2001	34	0
2002	16	0
2003	1	0
2004	2	0

---

widespread use of robust, virtually uncrackable encryption is one of the most difficult problems confronting law enforcement as the next century approaches... Law enforcement is in unanimous agreement that the widespread use of robust non-key recovery encryption ultimately will devastate our ability to fight crime and prevent terrorism. Uncrackable encryption will allow drug lords, spies, terrorists and even violent gangs to communicate about their crimes and their conspiracies with impunity."); See also http://www.wired.com/politics/law/news/2001/09/46816 ("Janet Reno, Clinton's attorney general, said in September 1999 that the new regulations struck a reasonable balance between privacy and security. 'When stopping a terrorist attack or seeking to recover a kidnapped child, encountering encryption may mean the difference between success and catastrophic failures.")

[31] A report by the U.S. Working Group on Organized Crime titled, ``Encryption and Evolving Technologies: Tools of Organized Crime and Terrorism,'' released in 1997, collected anecdotal case studies on the use of encryption in furtherance of criminal activities in order to estimate the future impact of encryption on law enforcement. The report noted the need for "an ongoing study of the effect of encryption and other information technologies on investigations, prosecutions, and intelligence operations."

[32] Public Law 106-197 amended 18 U.S.C. § 2519(2)(b) in 2001 to require that reporting should reflect the number of wiretap applications granted in which encryption was encountered and whether such encryption prevented law enforcement officials from obtaining the plain text of the communications intercepted pursuant to the court orders.

[33] See, *Wiretap Reports*, Administrative Office of the Courts, 2000-2009, available at http://www.uscourts.gov/Statistics/WiretapReports.aspx

[34] This does not mean that individuals investigated by law enforcement agencies are not using encryption. The reporting requirements only document instances in which encryption is encountered during intercept orders, not, for example, during the search of a suspect's home. As explained later in this article, law enforcement agencies conduct very few intercepts of computers or Internet traffic, and so it is not too surprising that they rarely encountering encryption.

2005	13	0
2006	0	0
2007	0	0
2008	2	0
2009	1	0

In 2010, as part of a new push for surveillance powers including encryption backdoors,[35] The FBI told one privacy advocate that the previously published encryption statistics were "mistaken." He was also told that that a forthcoming report would confirm that encryption remains a problem for law enforcement agencies.[36]

The number of wiretaps is increasing, primarily among state law enforcement agencies

Over the last decade, the use of electronic surveillance orders has increased nationwide, although this is largely due to a massive increase in use by the states. In 1987, there were 237 wiretap orders obtained by federal law enforcement agencies. One decade later, in 1997, there were 569, and by 2009, this had increased to 663. Over these twenty years, the number of federal wiretaps fluctuated, but generally increased. In contrast, there were 437 state wiretaps in 1987, which increased to 617 by 1997. It was in the decade that followed that states really embraced this surveillance method, as by 2009, the number jumped to 1713.

While all states have increased their use of wiretaps over time, California has embraced this technique more than any other state. In 1997, California law enforcement agencies rarely used wiretaps – just 28 in that year. By 2009, the number increased to 586, which is now more than any other state in the country. In contrast, New York law enforcement agencies obtained 304 wiretap orders in 1997, which gradually increased over the years to 424 orders in 2009.

These two states are now responsible for combined 58 percent of all state wiretap orders. Professor Paul Schwartz noted a similar trend several years ago, and observed that "[t]his pattern of use is likely

[35] Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, THE NEW YORK TIMES, Sep. 27, 2010, https://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=1 (last visited Apr 3, 2011)("Essentially, officials want Congress to require all services that enable communications … to be technically capable of complying if served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages.")

[36] http://arstechnica.com/tech-policy/news/2010/09/fbi-drive-for-encryption-backdoors-is-deja-vu-for-security-experts.ars ("Jim Dempsey, the West Coast director of the Center for Democracy and Technology, told Wired.com that the FBI is now saying that the numbers are mistaken—and they'll issue new ones in the spring.")

independent of crime patterns, but rather reflects local law enforcement practice norms, including prosecutorial familiarity with the complex set of legal requirements for obtaining wiretap orders."[37]

Non-content intercepts ("pen registers" and "trap and trace devices")

Pen register and trap and trace devices are used by law enforcement agencies to obtain non-content communications records in real-time, such as phone numbers dialed, "to" and "from" information associated with email messages and the IP addresses of computers to which a suspect connects. With the Passage of the Pen Register Act in 1986, Congress required that annual statistical reports on the use of this surveillance method be compiled and submitted by the Attorney General .[38] These reporting requirements were subsequently expanded in 2000.[39] Describing his reasons for proposing the bill that successfully expanded the reporting requirements, Senator Leahy stated that:

> "As the original sponsor of ECPA, I believed that adequate oversight of the surveillance activities of federal law enforcement could only be accomplished with reporting requirements such as the one included in this law."[40]

It is unclear from the legislative history why Congress opted to give the Attorney General the responsibility for compiling these reports and not the Administrative Office of the US Courts, which after two decades of reliably producing the wiretap reports, would have been the obvious choice to produce similar reports for pen register and trap and trace surveillance. It is also unclear why Congress opted to limit the reports to law enforcement agencies within the Department of Justice. As a result of this decision, the reports do not detail surveillance conducted other federal law enforcement agencies, such as the Secret Service or by state and local law enforcement agencies.[41]

---

[37] Paul M. Schwartz, Reviving Telecommunications Surveillance Law, 75 U. Chi. L. Rev. 287, 292 (2008).

[38] 18 U.S.C. § 3126 (2006); [38] S. REP. 99-541, S. Rep. No. 541, 99TH Cong., 2ND Sess. 1986, 1986 U.S.C.C.A.N. 3555, 1986 WL 31929 (Leg.Hist.)

[39] The expanded reports must include (1) The period of interceptions authorized by each order; (2) the number and duration of any extensions of the order; (3) the offense specified in the order or application or extension of the order; (4) the number of investigations involved; (5) the number and nature of the facilities affected; and (6) the identity, including district, of the applying investigative or law enforcement agency making the application and the person authorizing the order.

[40] 145 Cong. Rec. 31,311 (1999) (statement of Sen. Leahy).

[41] Not all states have wiretap authority. FIXME.

Although the pen register and trap and trace reports were intended to inform both the general public as well as Congress about the use and scale of these surveillance techniques,[42] Professor Paul Schwartz notes that that "Pen Register Act reports are not publicly available and generally disappear into a congressional vacuum."[43] While the Administrative Office of the US Courts has distributed the wiretap reports via its website since at least 1998, copies of pen register reports have only seen the light of day through the work of privacy advocates.[44] In 2010, the Department of Justice established a policy of proactively posting copies of the pen register reports to its website.[45]

Furthermore, in spite of a legal requirement to do so, the Department of Justice has repeatedly failed to submit the pen register and trap and trace reports to Congress on an annual basis. In 2004, the Department of Justice sent a single "document dump" to Congress, which included reports for the years 1999 through 2003.[46] There are no records available that indicate that the Department of Justice submitted any more reports to Congress until 2009, when it sent over another document dump, this time containing the reports for the years 2004 through 2008.[47] However, in 2010, a DOJ official told me

[42] "In this way, the Congress and the public will be informed of those jurisdictions using this surveillance technique—information which is currently not included in the Attorney General's annual reports." 145 Cong. Rec. 31,311 (1999) (statement of Sen. Leahy)

[43] Paul M. Schwartz, Reviving Telecommunications Surveillance Law, 75 U. Chi. L. Rev. 287, 296 (2008).

[44] Statistics for the years 1994 to 1998 were obtained by a staff attorney at the Electronic Privacy Information Center (EPIC) with contacts in Congress. See Approvals for Federal Pen Registers and Trap and Trace Devices 1987–1998, EPIC, online at http://www.epic.org/privacy/wiretap/stats/penreg.html; The Electronic Frontier foundation obtained copies of the reports for the years 1999-2003 through a Freedom of Information Act requests. Even then, DOJ took over three years to respond to this request and release the reports See: Letter to Kevin Bankston from Rena Y. Kim, Chief, FOIA Unit, Office of Enforcement Operations, Criminal Division, Department of Justice, June 5, 2008, *available at* http://files.spyingstats.com/pr-tt/doj-details-pr-tt-1999.pdf; I was able to obtain copies of the reports for 2004-2009 through Freedom of Information Act requests.

[45] Email from Nancy Libin, Chief Privacy & Civil Liberties Officer, Office of the Deputy Attorney General, Department of Justice to Christopher Soghoian, Oct. 13 2010, on file with author ("The 2008 and 2009 reports are posted here under "Frequently Requested Records." The Department will post them here annually as a matter of course whenever they become available.").

[46] Paul M. Schwartz, Reviving Telecommunications Surveillance Law, 75 U. Chi. L. Rev. 287 at 297 (2008).

[47] Letter from William Moschella, Assistant Attorney General, to Congressman John Conyers, Jr, et al., Nov. 3, 2004. Letter from Ronald Weich, Assistant Attorney General, to Congressman John Conyers, Jr, et al., October 29, 2009. See also Email from Nancy Libin, Chief Privacy & Civil Liberties Officer, Office of the Deputy Attorney General, Department of Justice to Christopher Soghoian, Sept. 3 2010, on file with author ("It is true that DOJ did not produce[] them annually but rather submitted them in bulk in 2004 and then again in 2009, as you said.").

that the Department had recently instituted policies designed to ensure that the reports would be submitted in the future.[48]

Finally, as Professor Schwartz has noted, "[t]he reports also fail to detail all of the information that the Pen Register Act requires to be shared with Congress."[49] The reports do not identify the district or branch office of the agencies that submitted the pen register and trap and trace requests, information required by 18 U.S.C. § 3126(8), and some reports also do not detail the offenses for which the pen register and trap and trace orders were obtained, as required by 18 U.S.C. § 3126(2).[50]

Analysis of existing reports

As these reports do not include data on the use of non-content intercepts by state or federal law enforcement agencies outside the Department of Justice, it is impossible to determine their true scale. [51] Even with these significant flaws, the Pen Register Act reports do reveal some interesting information, such as the massive growth in the use of these surveillance orders.

In 1987, the first year for which data exists, there were 1682 pen register and 97 trap and trace orders obtained by agencies within the Department of Justice.[52] Eleven years later, the number of pen registers nearly tripled to 4886, and the number of trap and traces increased nearly 25 times to 2437. In 1999, the reports started to provide numbers for specific federal agencies, and revealed , for example, that the FBI and DEA were each responsible for approximately half of the 4949 pen registers obtained that year, while the FBI alone was responsible for more than 84 percent of the 1553 trap and traces obtained.

---

[48] Libin email Sept 3 2010 (earlier footnote) ("I've checked with leadership in the Office of Legislative Affairs and the Criminal Division. Please bear in mind that new leadership took over the Office of Leg Affairs in 2009 and was not responsible for the failure to produce the reports in 2004-2008. They have put in place a process to make sure that the reports are submitted to Congress annually, as required by statute.")

[49] Schwartz at 297.

[50] Letter from Marc Rotenberg et al to Senators Leahy, http://epic.org/privacy/wiretap/ltr_pen_trap_leahy_final.pdf at page 3.

[51] Based upon the larger number of state wiretaps than federal wiretaps each year (1713 compared to 663 in 2009), it seems reasonable to assume that there are at least as many pen register and trap and trace orders obtained by state law enforcement agencies as those by federal agencies. It is quite likely that there are several times more state requests.

[52] The available reports covering 1987 through 1998 do not detail numbers for particular agencies within the Department of Justice. See Approvals for Federal Pen Registers and Trap and Trace Devices 1987-1998, Electronic Privacy Information Center, available at http://epic.org/privacy/wiretap/stats/penreg.html.

Although the numbers have fluctuated in particular years,[53] over time, the number of requests has skyrocketed. By 2009, the latest year for which statistics exist, 12,444 pen registers and 11,091 trap and trace orders were issued.[54] As such, this surveillance method vastly outnumbers wiretaps – in 2009, there were 18 times more pen registers than federal wiretaps. This difference might be because each of the 663 Federal intercept orders (described as "superwarrants" by some experts[55]) obtained in 2009 had to be thoroughly evaluated and then approved by a judge, while the 12,444 pen registers requests only received a cursory review at best.[56]

It is possible to observe a few other trends by analyzing the reports.

Between 1999-2008, the statistics reflect that the Drug Enforcement Administration (DEA) requested a single order for each person whose telephone facilities were affected.[57] However, in 2009, the DEA started monitoring multiple individuals with a single order (obtaining 3735 pen register orders for 4527 people, and 2995 trap and trace orders for 3434 people). Furthermore, between 1999 and 2006, the DEA got an order of magnitude more pen registers than trap and trace devices. In 2007, something changed as the DEA started to apply for similar numbers of orders. That year, the number of trap and trace orders sought by the DEA jumped 1700 percent from 148 the previous year to 2510.

Like the DEA, the US Marshals Service also appears to request a single order for each person monitored (at least for the years 2001-2009). However, the statistics also reveal that the agency obtains identical numbers of pen registers and trap and trace orders. Since the legal process required to obtain a pen register is the same as a trap and trace, this suggests that the "boilerplate" language used by the Marshals requests both as a matter of standard policy.

Starting in 2004, the reports also provide data on the use of non-content intercepts for email and network traffic. These numbers remain low, starting at just 20 pen registers in 2004 (obtained by the

[53] One interesting trend worth highlighting though is that the number of pen registers and trap & trace orders went down after 9/11 (4210 pen registers were used in 2000, 4172 in 2001, and 4103 in 2002), at a time when the FBI and other parts of DOJ were presumably opening large numbers of new investigations. One likely explanation for this is that federal investigators switched to other types of surveillance orders (such as those issued by the FISA court).

[54] See: http://files.spyingstats.com/pr-tt/DOJ-pen-registers-2004-2008.pdf

[55] http://intelligence.senate.gov/050419/kerr.pdf

[56] See 18 U.S.C. § 3123(a)(1). See *In re Application of United States*, 846 F. Supp. 1555, 1559 (M.D. Fla. 1994) ("The court will not conduct an 'independent judicial inquiry into the veracity of the attested facts.'"). See also *United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995) ("The judicial role in approving use of trap and trace devices is ministerial in nature.")

[57] In contrast, the report reveal that FBI monitors multiple individuals with each pen register order.

DEA), and eventually increasing to 258 pen registers and 50 trap and trace orders obtained by four different federal law enforcement agencies in 2009.[58]

Emergency voluntary disclosures

When Congress passed the Electronic Communications Privacy Act in 1986, it permitted law enforcement agencies to obtain stored communications and customer records in emergencies without the need for a court order.

In such scenarios, a carrier *can* (but is not required to) disclose the requested information if it, "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[59] Typically, belief means that a police officer states that an emergency exists.[60]

With the passage of the USA PATRIOT Improvement and Reauthorization Act of 2005, Congress created specific statistical reporting requirements for the voluntary disclosure of the contents of subscriber communications in emergency situations. In describing his motivation for introducing the requirement, Senator Lungren stated that:

> "I felt that some accountability is necessary to ensure that this authority is not being abused… This information [contained in the reports] I believe should be highly beneficial to the Committee, fulfilling our oversight responsibility in the future … this is the best way for us to have a ready manner of looking at this particular section. In the hearings that we had, I found no

[58] The DEA obtained 20 email/network pen registers in 2004, and 24 in 2005, 37 in 2006, 84 in 2007, 59 in 2008, and 56 in 2009. The DEA also obtained 47 trap and trace orders in 2009. The USMS obtained 61 pen registers in 2007, 79 in 2008, and 140 in 2009. The ATF obtained 5 pen registers and 3 trap and trace orders in 2009. Finally, the FBI obtained 59 pen registers and 45 trap and trace orders in 2008, and 57 pen registers and 52 trap and trace orders in 2009.

[59] See: 18 U.S.C. § 2702(b)(8) and 18 U.S.C. § 2702(c)(4) (discussing the production of information in emergency situations).

[60] See, e.g., Seth Rosenbloom, Crying Wolf in the Digital Age: Voluntary Disclosure under the Stored Communications Act, 39 COLUM. HUM. RTS. L REV 529, 559–561 (2008); See also, DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS, 261 n.272 (Jan. 2010) (quoting H.R. Rep No. 107-497, at 12-13 (2002)), available at http://www.justice.gov/oig/special/s1001r.pdf ("The legislative history of a similar amendment to Section 2702(b)'s emergency voluntary disclosure provision for content information suggests that the belief standard was relaxed because communications service providers 'expressed concern to the Committee that the [reasonably believes] standard was too difficult for them to meet, and that as a result, providers may not disclose information relating to emergencies.'").

basis for claiming that there has been abuse of this section. I don't believe on its face it is an abusive section. But I do believe that it could be subject to abuse in the future and, therefore, this allows us as Members of Congress to have an ability to track this on a regular basis."[61]

As with the Pen Register Act reports, the emergency request reports are compiled and submitted by the Attorney General, and only apply to disclosures made to law enforcement agencies within the Department of Justice. As such, there are no statistics for emergency disclosures made to other federal law enforcement agencies, such as the Secret Service, as well as those made to state and local law enforcement agencies.

Furthermore, although 18 USC 2702 permits both the disclosure of the content of communications, as well as non-content records associated with subscribers and their communications, Congress only required that statistics be compiled for the disclosure of communications content. It is not clear why Congress limited the reports in this way.

Analysis of existing reports

Because the reporting requirements do not apply to disclosures made to law enforcement agencies outside the Department of Justice, and do not include the disclosure of non-content communications data and other subscriber records, the reports reveal a very limited portion of the scale of voluntary disclosures to law enforcement agencies.

Furthermore, although Congress intended for these reports to assist with public oversight of the emergency disclosure authority, the Department of Justice has not proactively made these reports available to the general public. In spite of this lack of transparency by DOJ, three years of reports have been obtained by privacy advocates, and placed online.[62]

[61] http://www.gpo.gov/fdsys/pkg/CRPT-109hrpt174/pdf/CRPT-109hrpt174-pt1.pdf available at ; http://thomas.loc.gov/cgi-bin/cpquery/2?&sid=cp109EDBl7&refer=&r_n=hr174p1.109&db_id=109&item=2&&sid=cp109EDBl7&r_n=hr174p1.109&dbname=cp109&hd_count=2&item=2&&sel=TOC_247686& ("To address concerns that [the voluntary emergency disclosure] authority, in certain circumstances, is not subject to adequate congressional, judicial or public oversight … The Committee believes this would strengthen oversight on the use of this authority without undermining important law enforcement prerogatives, and without tipping off perpetrators while simultaneously preserving the vitality of this life saving authority.")

[62] The reports were provided to me by someone with connections in Congress. They have been placed online at http://www.spyingstats.com.

A letter submitted by Verizon to Congressional committees in 2007 revealed that the company had received 25,000 emergency requests during the previous year.[63] Of these 25,000 emergency requests, just 300 requests were from the federal law enforcement agencies. In contrast, the reports submitted to Congress by the Attorney General reveal less than 20 disclosures per year.[64] Even though no other service provider has disclosed similar numbers regarding emergency disclosures, it is quite clear that the Department of Justice statistics are not adequately reporting the scale of this form of surveillance. In fact, they underreport these disclosures by several orders of magnitude.

Section III: Unreported surveillance methods

The previous section analyzed the use of electronic surveillance as documented in official government reports. There are several other forms of electronic surveillance for which no official reports exist. As such, the little available data largely comes from the companies themselves. Unfortunately, many companies, particularly those with the close ties to the government, will not discuss their disclosure of user data to law enforcement agencies. The reason for this widespread secrecy appears to be a fear that such information may scare users and give them reason to fear that their private information is not safe.[65]

---

[63] Letter from Randal S. Milch, Sr. Vice Pres., Verizon Bus., to John D. Dingell, Edward J. Markey & Bart Stupak, U.S. Reps (Oct. 12, 2007), available at http://markey.house.gov/docs/telecomm/Verizon_wiretaping_response_101207.pdf

[64] The DOJ received voluntary disclosures from 17 accounts in 2006, 9 accounts in 2007, and from 17 accounts in 2008. Letter from Richard Hertling, Acting Assistant Attorney General, to Senator Patrick Leahy, April 9, 2007, available at http://files.spyingstats.com/exigent-requests/doj-2702-report-2007.pdf. Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney General, to Senator Patrick Leahy, April 24, 2008, available at http://files.spyingstats.com/exigent-requests/doj-2702-report-2008.pdf. Letter from Ronald Reich, Assistant Attorney General, to Senator Patrick Leahy, July 24, 2009, available at http://files.spyingstats.com/exigent-requests/doj-2702-report-2009.pdf.

[65] Ryan Singel, *Google, Microsoft Push Feds to Fix Privacy Laws*, WIRED (Mar. 30, 2010, 4:38 PM), *available at* http://www.wired.com/threatlevel/2010/03/google-microsoft-ecpa ("We [Microsoft] would like to see more transparency across the industry … But no one company wants to stick its head up to talk about numbers."); Letter from Michael T. Gershberg, Counsel to Yahoo! Inc, to William Bordley, U.S. Marshals Service (Sept. 15, 2009), *available at* http://files.cloudprivacy.net/yahoo-price-list-letter.PDF. ("[Surveillance pricing] information, if disclosed, would be used to 'shame' Yahoo! and other companies -- and to "shock' their customers. Therefore, release of Yahoo!'s information is reasonably likely to lead to impairment of its reputation for protection of user privacy and security, which is a competitive disadvantage for technology companies.")

Requests to service providers for stored communications and subscriber records

The Stored Communications Act enables law enforcement agencies to obtain stored communications and subscriber records. This includes stored emails, instant messages, web browsing history, search engine records as well as documents stored "in the cloud." There no official statistics regarding such requests, although based on publicly available information, they likely number in the tens of thousands per year.

AOL was the first company to voluntarily disclose statistics, revealing to the New York Times in 2006 that it received 1000 requests per month.[66] In 2009, a representative from Facebook told Newsweek that it was receiving between ten to twenty requests from police per day.[67] In response to a copyright lawsuit in 2010, Time Warner revealed that it received approximately 500 IP address lookup requests for associated with its cable customers on average per month, nearly all of which came from law enforcement.

In April 2010, Google started publishing statistics regarding the number of requests for user data the company receives from governments around the world. According to those reports, the company received 4287 requests for user data between January 2010 to June 2010, and 3580 requests between July 2009 and December 2009. The company has not broken down these numbers into the various types of requests it receives.[68]

---

[66] Hansel, supra note FIXME ("AOL, for example, has more than a dozen people, including several former prosecutors, handling the nearly 1,000 requests it receives each month for information in criminal and civil cases. . . . AOL says that only 30 of the 1,000 monthly requests it receives are for civil cases, and that it initially rejects about 90 percent of those, arguing that they are overly broad or that the litigants lack proper jurisdiction. About half of those rejected are resubmitted, on narrower grounds.").

[67] Nick Summers, Walking the Cyberbeat, NEWSWEEK, May 18, 2009, available at http://www.newsweek.com/id/195621 ("[Facebook] says it tends to cooperate fully and, for the most part, users aren't aware of the 10 to 20 police requests the site gets each day."). However, consider that Facebook had 200 million users in 2009, and now has more than 600 million. As such, it is probably reasonable to assume that it probably now receives many more requests.

[68] http://www.google.com/transparencyreport/faq/#removalrequests ("The number of requests we receive for user account information as part of criminal investigations has increased year after year. The increase isn't surprising, since each year we offer more products and services, and we have a larger number of users … At a time when increasing numbers of governments are trying to regulate the free flow of information on the Internet, we hope this tool will shine some light on the scale and scope of government requests to … obtain user data around the globe – and we welcome external debates about these issues that we grapple with internally on a daily basis.")

In 2010, Congress held several hearings to examine the 20 year-old Electronic Communications Privacy Act. Republican Senators dismissed entirely the pleas of both companies and privacy advocates to protect communications content stored "in the cloud," by arguing, anecdotally, that the vast majority of requests for stored content are for child pornography investigations.[69] These claims were stated in a minority staff report, by an anonymous former federal prosecutor, citing his own experience at the Department of Justice. Because no official statistics exist, there is no way to verify this claim. However, it is worth noting that the majority use of most other forms of surveillance is to investigate drugs, not child pornography.

[69] Memorandum to the SJC Minority Staff, The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age, Sept 17, 2010 at page 8 ("As noted above, anecdotally, a substantial majority of ECPA orders are used in child exploitation cases, meaning that the primary direct beneficiary of the changes proposed by Digital Due Process will be this class of offenders. In these cases, prosecutors are not usually interested in the content of communications; they are interested in quickly locating offenders in order to apprehend them to protect children.") *available at* http://www.scribd.com/doc/38407733/Republican-Senate-memo-against-privacy-and-cloud-computing-reform

Surveillance of location information

Law enforcement requests for location information from wireless carriers, both historical and real-time ("prospective") have become routine.[70] Each wireless carrier reportedly receives "thousands" of requests per month, an amount that has grown "exponentially" over the past few years.[71] According to 9th Circuit Chief Judge Alex Kozinski, "[t]he volume of requests [received by wireless carrier Sprint Nextel] grew so large that the 110-member electronic surveillance team couldn't keep up, so [in 2008,] Sprint automated the process by developing a web interface that gives agents direct access to users' location data."[72] That website was used by law enforcement agents to "ping" Sprint users over 8 million times in a single year.[73]

In addition to requesting this data from wireless carriers, law enforcement agencies are also able to directly collect prospective phone location data using specialized equipment known as a cell site simulator or "triggerfish."[74] Just as with requests to carriers for location data, no statistics exist regarding the use of this covert location tracking technique.

---

[70] Ellen Nakashima, *Cellphone Tracking Powers on Request*, The Washington Post, November 23, 2007. ("Federal officials are routinely asking courts to order cellphone companies to furnish real-time tracking data so they can pinpoint the whereabouts of drug traffickers, fugitives and other criminal suspects, according to judges and industry lawyers."); Christopher Guttman-McCabe, vice president of regulatory affairs for CTIA -- the Wireless Association, in a July 2007 comment to the Federal Communications Commission ("Law enforcement routinely now requests carriers to continuously 'ping' wireless devices of suspects to locate them when a call is not being made ... so law enforcement can triangulate the precise location of a device and [seek] the location of all associates communicating with a target."); Declan McCullagh, Feds push for tracking cell phones, CNET News, Feb. 11, 2010, available at http://news.cnet.com/8301-13578_3-10451518-38.html ("'Obtaining location details is now "commonplace,' says Al Gidari, a partner in the Seattle offices of Perkins Coie who represents wireless carriers. 'It's in every pen register order these days'").

[71] Michael Isikoff, *The Snitch in Your Pocket*, NEWSWEEK, Feb. 19, 2010, available at http://www.newsweek.com/2010/02/18/the-snitch-in-your-pocket.html (telecom lawyer Al Gidari describing the scale of location requests received by wireless carriers).

[72] *US v. Pineda-Moreno*, 617 F. 3d 1120 - Court of Appeals, 9th Circuit 2010 – dissent by Kozinski at 1125

[73] Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, SLIGHT PARANOIA (Dec 1, 2009) *available at* http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html.

[74] USABook -> Electronic Surveillance -> Cell Site Simulators, Triggerfish, Cell phones. Page 18, available at, http://www.aclu.org/pdfs/freespeech/cellfoia_release_074130_20080812.pdf (Triggerfish can be deployed "without the user knowing about it, and without involving the cell phone provider."); Julian Sanchez, *FOIA docs show feds can lojack mobiles without telco help*, ARS TECHNICA, November 16, 2008, *available at* http://arstechnica.com/tech-policy/news/2008/11/foia-docs-show-feds-can-lojack-mobiles-without-telco-help.ars ("The Justice Department's electronic surveillance manual explicitly suggests that triggerfish may be used to avoid restrictions in statutes like CALEA that bar the use of pen register or trap-and-trace devices—

In 2000, the Republican controlled House of Representatives considered legislation that would set clear standards governing requests for location data. The same bill included a requirement that statistical reports be created for location data and requests to internet service providers. The Department of Justice opposed the bill, stating that the additional reporting requirements would consume scarce resources and "threaten[ed] to turn crime-fighters into bookkeepers."[75] Ultimately, the bill did not make it out of committee.

A decade later, when the House again looked into the topic of government requests for location data, there were still no statistics related to this technique. Because it didn't pass any legislation mandating reporting of such requests, Congress in 2010 knew just as little as it did in 2000.

---

which allow tracking of incoming and outgoing calls from a phone subject to much less stringent evidentiary standards—to gather location data.").

[75] PREPARED STATEMENT OF KEVIN DIGREGORY, DEPUTY ASSOCIATE ATTORNEY GENERAL, DEPARTMENT OF JUSTICE, Hearing on "ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 2000, DIGITAL PRIVACY ACT OF 2000 AND NOTICE OF ELECTRONIC MONITORING ACT", September 6, 2000, http://commdocs.house.gov/committees/judiciary/hju67343.000/hju67343_0f.htm ("the imposition of such extensive reporting requirements for cyber-crime investigators would come at a time when law enforcement authorities are strapped for resources to fight cyber-crime. The reporting requirements for wiretaps, while extensive, are less onerous because law enforcement applies for such orders relatively rarely. Extending such requirements to orders used to obtain mere transactional data would dramatically hinder efforts to fight cyber-crime, such as the distribution of child pornography and Internet fraud.")

Section IV: Closing the surveillance reporting gap

Even without complete statistics, it is quite clear that many law enforcement agencies have enthusiastically embraced surveillance of stored communications and transactional records. While wiretaps, the "most carefully regulated and reported-on area of telecommunications surveillance"[76] are used just a few thousand times per year, law enforcement agencies now make tens (if not hundreds) of thousands of requests per year for subscriber records, stored communications and location data. Unfortunately, Congress lacks any statistical data regarding many of these requests, and so is largely unable to perform effective oversight over this surveillance power.[77]

In 2008, Professor Paul Schwartz suggested that Congress create an annual telecommunications surveillance index (a surveillance "report card"), instead of the "bits and pieces of scattered reports" released each year.[78] That suggestion remains a valid and useful one, but even if Congress does not create a single resource for surveillance statistics, there are several ways in which it can significantly enhance its own and the general public's awareness of modern electronic surveillance.

First, the Pen Register Act should be amended so reporting under it is made to the Administrative Office of the courts, rather than the Department of Justice. Since judges have to approve pen register orders, it should be simple enough for clerks to send this information to the Administrative Office, just as they already do for wiretap orders. The Pen Register Act should also be amended so that the reporting requirements apply to all law enforcement agencies, and not just those federal agencies within the Department of Justice. For example, if the Secret Service or Los Angeles Police Department obtains a pen register order, it should be reported.

Second, the emergency disclosure reports, like the Pen Register Act reports, should be expanded to include disclosures made to all law enforcement agencies, and not just those federal agencies within the Department of Justice. These reports should be sent directly to the Administrative Office of the Courts, which can then compile them and send them onto Congress as part of a broader surveillance report. The emergency disclosure reports should also be broadened to include emergency disclosures of non-content data and customer records.

Third, detailed statistics should be created regarding requests made to service providers for stored communications and subscriber data under the Stored Communications Act. When such disclosures are made pursuant to a court order, the courts should compile and transmit the information to the Administrative Office. However, because such disclosures can and are regularly made in response to a

[76] Schwartz at 310.

[77] Electronic Communications Privacy Act of 2000, HR Rep No 106-932, 106th Cong, 2d Sess 10 (2000) (lamenting that there was little data with which to understand the effects of the Electronic Communications Privacy Act of 1986).

[78] Schwartz at 313.

subpoena, additional reports will be necessary. Rather than requiring every law enforcement agency in the country to send reports to the Administrative Office, I propose that Internet Service Providers should be required to create and submit annual reports to the Administrative Office, which can then strip out the providers' identifying information, and compile reports that summarize the provider data.[79]

Fourth, Congress should create specific reporting requirements regarding the collection of historical and prospective location information, detailing the number of requests, the type of information requested, and the number of individuals whose information was obtained.

These reporting requirements would provide Congress with the information necessary to make sound policy in the area of electronic surveillance, yet because most of the responsibility for actually creating and compiling the reports falls upon the courts and the companies themselves, law enforcement agencies would not be able to complain, as they did in 2000, that the requirements would overburden them.[80]

In December 2010, a staffer working for the House Subcommittee on the Constitution, Civil Rights, and Civil Liberties circulated a draft discussion bill that included all four of these recommendations. Unfortunately, that bill was never formally introduced.

Section V: Conclusion

Law enforcement agencies have had the ability to covertly monitor the communications of Americans for nearly a century. In order to perform effective oversight over these powers, Congress required the creation of surveillance reports that document the use of wiretaps and later pen registers. However, as Americans have increasingly embraced modern technologies such as mobile phones and the Internet, law enforcement agencies have followed. Unfortunately, there are no reporting requirements for the modern surveillance methods that make up the majority of law enforcement requests to service providers and telephone companies. As such, this surveillance largely occurs off the books, with no way for Congress or the general public to know the true scale of such activities.

---

[79] It would be wise to include some *de minimis* rule, so that small providers that do not receive large numbers of requests would not be burdened with this requirement. Furthermore, since providers will incur costs associated with creating and submitting these reports, I suggest that they be permitted to seek reasonable compensation from the Administrative Office for doing so.

[80] PREPARED STATEMENT OF KEVIN DIGREGORY, DEPUTY ASSOCIATE ATTORNEY GENERAL, DEPARTMENT OF JUSTICE, Hearing on "ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 2000, DIGITAL PRIVACY ACT OF 2000 AND NOTICE OF ELECTRONIC MONITORING ACT", September 6, 2000 http://commdocs.house.gov/committees/judiciary/hju67343.000/hju67343_0f.htm (The reporting requirements "create a significant burden for law enforcement authorities…. The imposition of such extensive reporting requirements for cybercrime investigators at a time when law enforcement authorities are strapped for resources to fight cybercrime would hinder our efforts to fight cybercrime.")

In writing this article, I have tried to collect all publicly available information (as well as some not previously available) in order to present as complete a picture as possible regarding the current state of electronic surveillance. Even so, Congress should not have to rely on the work of a graduate student in order to keep tabs on this increasingly important issue. As demonstrated by the few pages of information presented in Section III, very little is known about the true scale of requests for stored communications or location data, although they likely number in the tens or hundreds of thousands per year.

In 2000, Congress considered legislation that would have significantly enhanced the surveillance reporting requirements. It failed to pass that bill. This year, Congress is again considering updating the aging Electronic Communications Privacy Act in order to better protect location data as well as data stored in the cloud. Unfortunately, Congress lacks independent, high-quality data upon which to evaluate law enforcement use of its existing surveillance powers.

If Congress punts on comprehensive privacy reform, as it has done so several times in the past, I hope that it at least mandates the creation of new surveillance statistics. Doing so will ensure that a future Congress will at least be equipped with useful data.