THE SPIES WE TRUST: THIRD PARTY SERVICE PROVIDERS AND LAW ENFORCEMENT SURVEILLANCE

Christopher Soghoian

Submitted to the faculty of the Graduate School

in partial fulfillment of the requirements

for the degree

Doctor of Philosophy

in the School of Informatics, Department of Computer Science

Indiana University

July 2012

Accepted by the Graduate Faculty, Indiana University, in partial fulfillment of the requirements of the degree of Doctor of Philosophy.

Doctoral Committee

Geoffrey Fox, Ph.D.
(Principal Advisor)

Markus Jakobsson, Ph.D.

Fred Cate, J.D.

Marc Rotenberg, J.D.

July 15, 2012

"The creatures outside looked from pig to man, and from man to pig, and from pig to man again; but already it was impossible to say which was which."

—GEORGE ORWELL, ANIMAL FARM

Acknowledgements

First, I would like to thank L. Jean Camp, who selflessly put herself at risk in order to save me from two extremely unpleasant encounters with the FBI. I will be indebted to her forever.

I would also like to thank Stephen Braga and Jennifer Granick, two stellar attorneys who came to my defense in 2006 after the FBI took an interest in my work, raiding my home at 2AM and seizing my personal documents and computers. Their expert assistance led to the return of my possessions in just three weeks and the closing of the FBI's criminal and TSA's civil investigations without any charges filed.

Jennifer Granick came to my assistance a second time (and was joined by Steve Leckar) in 2010 after the Federal Trade Commission's Inspector General investigated me for using my government badge to attend a closed-door surveillance industry conference. It was at that event where I recorded an executive from wireless carrier Sprint bragging about the eight million times his company had obtained GPS data on its customers for law enforcement agencies in the previous years.

I am immensely indebted to Al Gidari, who knows more about law enforcement surveillance than anyone else outside of the government. The breadcrumbs he has left behind have been more useful than any other single source of data.

I would also like to thank Kevin Bankston, David Sobel, Marcia Hoffmann and Catherine Crump, who were exposing and fighting government surveillance long before I took an interest in the topic. They helped me to learn the obscure art of the FOIA request, and inspired a number of my own requests, several of which have borne useful fruit. Nabiha Syed has also been extremely generous with her time, helping me with my clumsy efforts

to engage in *pro se* FOIA litigation.

I am, of course, not the only researcher or activist interested in Internet surveillance. Caspar Bowden, Ian Brown, Duncan Campbell, Eric King, Christopher Parsons, Aaron Martin, Julian Sanchez and Marcy Wheeler have done their own share of muckraking and expert analysis, pointing me to resources and critiquing my own theories.

Tim Sparapani, during his time working as a Washington lobbyist for Facebook, unintentionally taught me how to stand up to bogus legal threats from a large corporation. For this lesson, I thank him. I suspect that it will be a skill that will pay dividends in the future.

The stimulating conversations I've had with Paul Ohm have forced me to rethink my previously black and white view of the world, in which I demonized anyone who had at one point chosen to work for the Department of Justice, particularly in the area of computer crime.

Likewise, my friendship and collaboration with Stephanie Pell has been a wonderful surprise. I would have never expected to befriend a former national security prosecutor, let alone be repeatedly welcomed into her home. Stephanie has helped me to better understand the law enforcement perspective and forced me to be far more pragmatic in my interactions with people in Washington.

Jim Green introduced me to the Washington handshake, opened doors that I never knew existed and has been an absolutely fantastic mentor in the ways of Washington. I would have never predicted that I'd be able to find common ground with a telecom industry lobbyist, let alone be able to honestly describe him as a friend. This city can bring people together in strange ways.

I spent one year at the Federal Trade Commission, and thus have several people to thank there. While the agency's powers are often limited, Commissioner Pamela Jones Harbour was willing to use her bully pulpit to pressure companies to put privacy first.

She taught me that a single speech can be an extremely effective way to nudge industry to protect consumers, particularly when regulators have limited powers. I would also like to thank David Vladeck, Chris Olsen and the entire Division of Privacy and Identity Protection. My time at the FTC was by far the most rewarding, yet most frustrating year of my life thus far. I created constant headaches for management, and no doubt annoyed many people with my habitual lateness, my refusal to submit to the background check required of all federal employees, my shorts and sandals, and the flood of new cases I proposed. I greatly appreciate the patience and goodwill that everyone at the FTC showed me.

My research into government surveillance first began during a one-year fellowship at the Berkman Center, during which they gave me the impossible task of trying to measure the scale of government surveillance. Thankfully, they were not upset when I failed. As a member of the Berkman community, numerous doors have opened for me. For this, and the countless stimulating conversations I had during my year in Cambridge, I am very thankful.

I am immensely indebted to Paul Syverson, who, during an evening chat in Bloomington, gave me the best advice of my entire academic career. Had I not followed it, I am certain that I would not have lasted this long in academia.

Marc Rotenberg first introduced me to writing FTC complaints and using them to frame the policy debate. The path I now follow as a privacy activist in Washington DC is one that Marc played a major role in establishing and legitimizing. Watching him in action has been highly educational.

At the beginning of my graduate studies in Indiana, Fred Cate was critical, and reasonably so, of my reckless approach to activism and the lack of focus in my academic research. In the years since, he has become one of my strongest supporters, and, quite amusingly, has also become a vocal opponent of security theatre, long after I stopped harassing the

Transportation Security Administration.

Markus Jakobsson has been a fantastic academic advisor, who has been there for advice when I needed it, but hands off enough to let me find my own direction. Most surprising, he willingly remained my advisor long after my focus strayed away from our shared interest in phishing and fraud. Were it not for his support, and repeated prodding, I would never have finished.

Geoffrey Fox kindly volunteered to chair my dissertation committee after university rules prohibited Markus from continuing to formally occupy the role. In doing so, Geoffrey freed me from a nightmare of red tape, frustration, and numerous arguments with university officials.

Over the past several years, my activism and research have not been entirely focused on the issue of government surveillance. Derek Bambauer, Kelly Caine, Allan Friedman, Ashkan Soltani, Sid Stamm and Harlan Yu have helped me out countless times with many other privacy and security related projects.

Finally, over the last few years, a large number of individuals have leaked information to me. In some cases, these leaks were to score political points, to harm their competitors, or in a few cases, because they are alarmed by the government's actions or surveillance powers. Whatever the reasons, these leaks have been extremely helpful, and so while I cannot for obvious reasons name my sources, I would like to thank them here.

Christopher Soghoian

THE SPIES WE TRUST: THIRD PARTY SERVICE PROVIDERS AND LAW ENFORCEMENT SURVEILLANCE

Telecommunications carriers and service providers now play an essential role in facilitating modern surveillance by law enforcement agencies. The police merely select the individuals to be monitored, while the actual surveillance is performed by third parties: often the same email providers, search engines and telephone companies to whom consumers have entrusted their private data. Assisting Big Brother has become a routine part of business.

While communications surveillance is widespread, the official government reports barely scratch the surface. As such, the true scale of law enforcement surveillance has long been shielded from the general public, Congress, and the courts. However, recent disclosures by wireless communications carriers reveal that the companies now receive approximately one and a half million requests from U.S. law enforcement agencies per year.

In addition to forcing companies to disclose the user data they already have, companies are also regularly compelled to modify their products in order to facilitate government surveillance. Some have been required to build surveillance capabilities directly into their products, while others have been forced to repurpose existing features in commercial products for surveillance.

In spite of the government's ability to compel assistance, many companies have a surprising amount of freedom to design privacy enhancing features into their products, including minimal data retention policies and data encryption. Likewise, where the law is vague, companies can adopt strict, pro-privacy legal positions, forcing the government to obtain a warrant and providing users with notice when their data is disclosed to the police.

Although companies are able to build privacy protections into their products and embrace pro-privacy legal theories, few do so, and those that do, rarely discuss it. Significant differences exist regarding the extent to which service providers protect the privacy of their customers, yet there is no real way for consumers to learn these differences and compare providers. The market for privacy, at least with regard to government access, simply does not exist.

Contents

List of Tables

List of Figures

1

Introduction

> "Under ordinary and normal circumstances wiretapping by Government agents should not be carried on for the excellent reason that it is almost bound to lead to abuse of civil rights" [1].
>
> —PRESIDENT FRANKLIN D. ROOSEVELT,
> MEMORANDUM FOR THE ATTORNEY GENERAL, 1940

In the space of just a few years, American consumers and businesses have embraced cloud computing services, often coupled with smart mobile devices. Hundreds of millions of consumers have signed up for services and products offered by Google, Facebook, Twitter and others. Often, these services are provided at no direct financial cost. Instead, consumers pay for the services with their personal data [2]. This data is mined by the service providers and often used to deliver targeted advertising. Unsurprisingly, as users and their data have migrated to the cloud and mobile platforms, law enforcement agencies have followed.

Wiretaps, at least when portrayed by Hollywood, often involve government agents hiding in an unmarked van outside a suspect's home, headphones on, listening to phone conversations taking place inside [3]. Similarly, seizures of digital evidence seem to usually involve a pre-dawn raid by teams of armed officers, who later emerge victorious from a home with computers and boxes of storage media. And of course, in the movies, FBI agents and police officers obtain this evidence themselves, usually at great personal risk.

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, mobile phones and the shift to cloud computing. The police no longer have to scale telephone poles in order to tap lines. Instead, most modern surveillance can be performed with a few clicks of a mouse, a fax, or a phone call to a service provider, all from the comfort and safety of the officer's desk [4]. The police merely select the individuals to be monitored, while the actual surveillance is performed by third parties: often the same email providers, search engines and telephone companies to whom consumers have entrusted their private data. Collectively, these companies now receive approximately one and a half million requests from U.S. law enforcement agencies per year,[1] which are processed by dedicated electronic surveillance and legal compliance departments [5]. As a result, assisting Big Brother has become a routine part of business, albeit one that some service providers would probably rather do without [6].

The central role that service providers now play in the surveillance of their customers significantly impacts both its scale and efficiency. Specifically, law enforcement agencies now have access to sources of data that didn't exist in the past, can obtain users' data without their knowledge, with less effort and at lower cost, and often, without any independent judicial review. At the same time, due to the covert nature of most investigations, these companies are often the only proxy capable of standing between their customers' data and the government,[2] even though the companies and their customers may have differing incentives.

Although service providers facilitate most modern surveillance, this is a position that

[1] An explanation for this estimate is presented in chapter 2.

[2] At a House Judiciary Committee hearing in 2011, Congressman Robert C. Scott asked Todd Hinnen, Acting Assistant Attorney General for National Security at the Department of Justice "why would [a service provider] ... have an incentive to hire lawyers to protect [their subscribers' privacy] rights?" Mr. Hinnen responded by stating his belief that "telecommunication providers and Internet service providers take the privacy of their customers and subscribers very seriously and I think are often an effective proxy for defending those rights" [7].

few are comfortable with [8], and none advertise [9]. The large communications companies claim that they are caught "between a rock and a hard place" [6]. Assistance is expected and demanded by law enforcement agencies, yet privacy advocates publicly shame, and in some cases, sue those companies that go out of their way to assist the government.[3]

In short, telecommunications carriers and service providers play an essential role in facilitating modern surveillance. In spite of this, there is little existing academic research that analyzes service providers and their role in the modern surveillance state. This lack of published research is not surprising — there is little relevant data in the public record, companies are often unwilling to talk about the topic, and law enforcement agencies do not want the general public (including criminals) to understand the true extent of their surveillance capabilities and limits. The goal of my research has been to change that, primarily in order to enable an informed public debate about the critical role that service providers play in facilitating surveillance of their customers.

Over the past several years, I have made extensive use of the Freedom of Information Act, filed a lawsuit seeking records from the Department of Justice, and cultivated source relationships within several major service providers. Through these and other research methods, I have been able to obtain a large quantity of original data which I present and analyze in this dissertation in order to shed light on the complex relationship between service providers and law enforcement agencies.[4]

This dissertation is arranged as follows: In chapter 2, I analyze the scale of modern electronic surveillance, revealing what is known about the number of requests made to third party service providers by law enforcement agencies. In chapter 3, I explore the ways in which companies are forced either build new surveillance technologies into their

[3] *See Hepting v. AT&T*, 439 F. Supp. 2d 974 (N.D. Cal. 2006) and *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 671 F.3d 881 (9th Cir. 2011).

[4] Intelligence agencies can and do regularly obtain user data from service providers. However, this dissertation is focused solely on the electronic surveillance conducted by law enforcement agencies. While I am also interested in the intelligence agencies, it is largely impossible to learn much useful information about that topic due to its classified nature.

products, or to repurpose existing features for surveillance. In chapter 4, I explore the economics of modern surveillance, focusing on the degree to which companies can and do charge for the assistance they provide, and further, the extent to which charging for surveillance assistance can protect users' privacy. In chapter 5, I explore the specific technologies implemented by companies to protect the privacy of their users and to limit the ability of the government to obtain their data. In chapter 6, I present several pro-privacy legal theories adopted by companies to shield their customers' communications from the government. In chapter 7, I delve into the failed market for privacy, and seek to explain why companies do not visibly compete on the degree to which they protect their customers from government surveillance. In chapter 8, I describe several areas of future work, and in chapter 9, I conclude.

Part I

The Government

"The telephone has become part and parcel of the social and business intercourse of the people of the United States, and the telephone system offers a means of espionage compared to which general warrants and writs of assistance were the puniest instruments of tyranny and oppression."

—BRIEF FOR PACIFIC TELEPHONE AND TELEGRAPH COMPANY ET AL.
OLMSTEAD V. UNITED STATES, 277 U.S. 438 (1928)

"The progress of science in furnishing the government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."

—JUSTICE LOUIS BRANDEIS, DISSENT IN OLMSTEAD V. UNITED STATES

2

The frequency of law enforcement access to user data

> "How many phone records are captured every year, anybody have a clue? Anybody know what happens to them when they're captured? How many times are cell phones pinged by the government every day, anybody know? Anybody know what happens to that location when it is captured? How about your emails, anybody know? We have an absolute absence of data and yet we're going to ask Congress to make decisions on what the appropriate [legal] standards are" [10].
>
> —AL GIDARI, A SURVEILLANCE LAW EXPERT RETAINED BY MANY LARGE COMPANIES

Third party facilitated surveillance has become a routine tool for U.S. law enforcement agencies, enough so that major providers like AT&T, Verizon, Google and Facebook all have dedicated teams [11, 12] who collectively receive and respond to approximately one and a half million requests each year.[5] While this practice is common, there is little public data quantifying the degree to which companies are forced to spy on their customers. As such, the true scale of law enforcement surveillance, although widespread, remains largely shielded from Congress, the general public and the courts [13, 14].[6]

[5] There are no official statistics that detail the number of law enforcement requests received by service providers. However, major wireless telecommunications companies have disclosed aggregate statistics which support this estimate. These statistics are discussed later in this chapter.

[6] This chapter analyzes the public reports on law enforcement surveillance methods. There also exist public reports on the use of some surveillance powers by intelligence agencies [15]. However, the scale of intelligence agencies' surveillance is beyond the scope of this dissertation.

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 ("wiretaps") and non-content, metadata records ("pen registers" and "trap and trace devices"). In order to enhance its oversight of these surveillance powers, Congress mandated that annual reports be created documenting their use.[7]

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 surveillance methods and sources of data for which there are no mandatory reporting requirements, such as requests for subscriber information, call records, stored emails, search engine queries, and geo-location information. As a result, most modern surveillance methods, which by conservative estimates vastly outnumber traditional wiretaps and pen registers, take place entirely off the books.[8]

2.1 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 involving the real-time interception of communications data. This section will explore each of these law enforcement surveillance powers and examine specific trends detailed in the reports.

[7] These reports were 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" [16].

[8] For example, according to a letter sent by a Verizon executive to members of Congress in 2007, the company received approximately 90,000 requests from law enforcement agencies in 2006 [17]. 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 [18] and the approximately 2300 wiretap orders issued nationwide in 2009 [19].

2.1.1 Electronic intercepts of communications content

In 1968, Congress established federal rules governing the use of real-time electronic interception. This law, the Omnibus Crime Control and Safe Streets Act, also required the Administrative Office of the U.S. Courts to compile and submit to Congress detailed annual reports on the use of wiretaps by law enforcement agencies.[9] The legislative history for the Act states that:

> "[The wiretap reports] are intended to form the basis for a public evaluation of its operation . . . [they] will assure the community that the system of court-order electronic surveillance . . . is properly administered " [20].

The Administrative Office of the U.S. Courts has published these reports and made them available on its website since 1997 [19].[10] By comparing the reports, several trends can be observed 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 1968 and 2011, law enforcement agencies obtained 46,988 wiretap orders. Requests have increased each year: In 1968, there were 174 wiretap orders authorized nationwide; ten years later, the number increased to 570; by 2000, there were 1,190 wiretaps; and in 2011, the most recent year for which reports exist, 2,732 wiretaps were authorized.[11]

[9] The reports are extremely detailed, and for each wiretap, reveal the city or county where the order was issued; the kind of interception (landline, mobile phone, computer, etc.); 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.

[10] The complete reports for the years 1968 to 1996 are not available online. However, the Electronic Privacy Information Center has published a summary of orders authorized and denied for the years 1968–1985 [21].

[11] As Julian Sanchez has observed, a significant percentage (twenty-eight percent in 2008, for example) of the wiretaps authorized each year are not included in the annual reports, as they were not reported to the Administrative Office of the U.S. Courts until after the filing deadline. According to Sanchez, "the number that makes it into the headlines is consistently 600-700 wiretap orders short, compared with the amended numbers quietly released years later" [22].

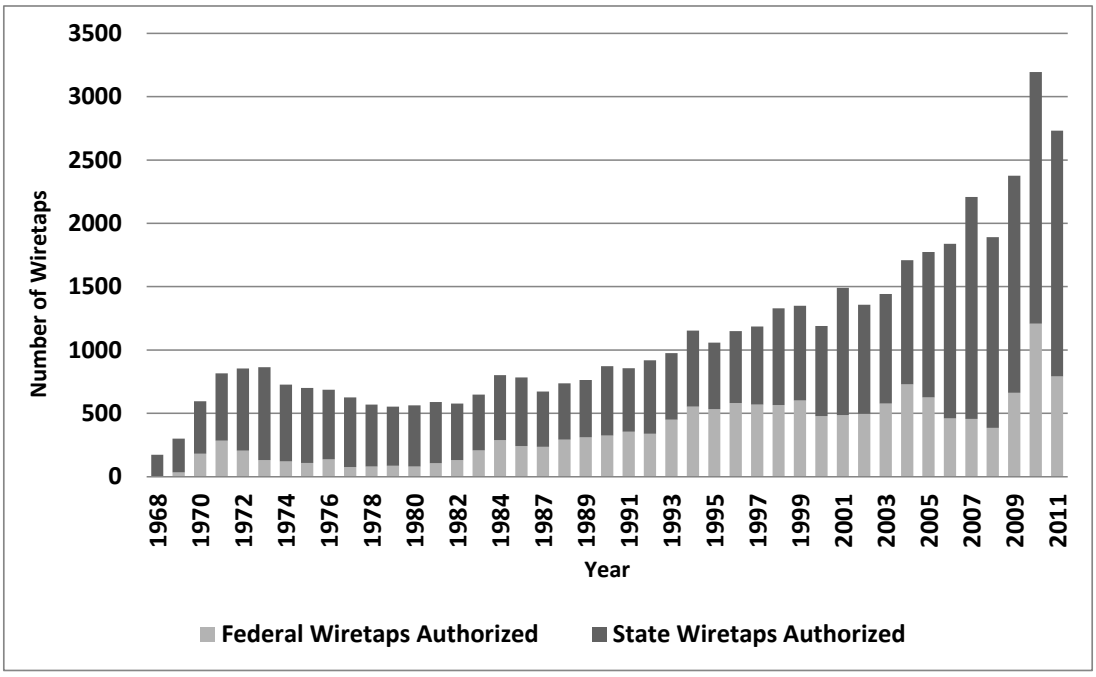

Figure 2.1: Wiretap Orders Approved by Federal and State Courts, 1968–2011

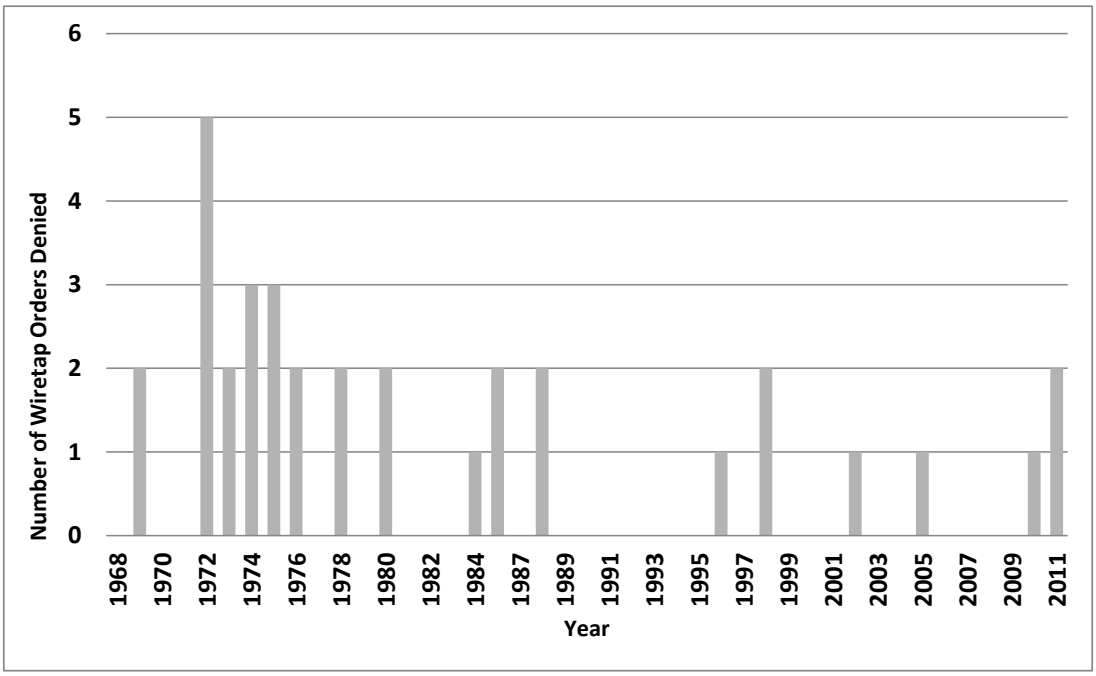

Figure 2.2: Wiretap Orders Denied by Courts Nationwide, 1968–2011

Over the past four decades, requests for wiretap orders have been rejected just 34 times by federal and state courts. The low number of rejections is not particularly encouraging, and might suggest that courts are rubber stamping wiretap requests.[12] However, Professor Paul Ohm offers an alternate explanation: the high approval rate for federal wiretap orders likely reflects vigorous internal quality controls within the Office of Enforcement Operations at the Department of Justice [23].[13] 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, more than 97 percent of the 2,732 wiretaps authorized in 2011 were for portable devices. As described earlier, the number of wiretaps has gone up each year over the past few decades. The statistics in the wiretap reports suggest that this increase is largely due to increases in the number of mobile devices monitored.[14]

There are several factors that may explain this trend. First, our society has increasingly "cut the cord" by switching to mobile phones [25]. It is understandable that law enforcement agencies have followed their targets to this new technology. This trend is more pronounced among young people and the poor, both of whom are generally more likely to be subject to investigation by the government [26]. 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 telephone exchange.[15]

[12]Similarly, the Second Circuit Court of Appeals cited the almost one hundred percent approval rate of the FISA Court in suggesting that there is insufficient oversight of electronic surveillance conducted by intelligence agencies. *See Amnesty International USA v. Clapper*, 638 F.3d 118, 2nd Circuit (2011).

[13]According to Deputy Attorney General James M. Cole, the Office of Enforcement Operations (OEO) is "primarily responsible for the Department's statutory wiretap authorizations." Lawyers in OEO review wiretap applications to ensure that they "meet statutory requirements and DOJ policies" [24].

[14]In 1997, there were 382 residential wiretaps, 78 at places of business, 185 for multiple locations, and 529 "other" (a catch-all category that included early mobile devices). In 2011, there were 13 residential wiretaps,

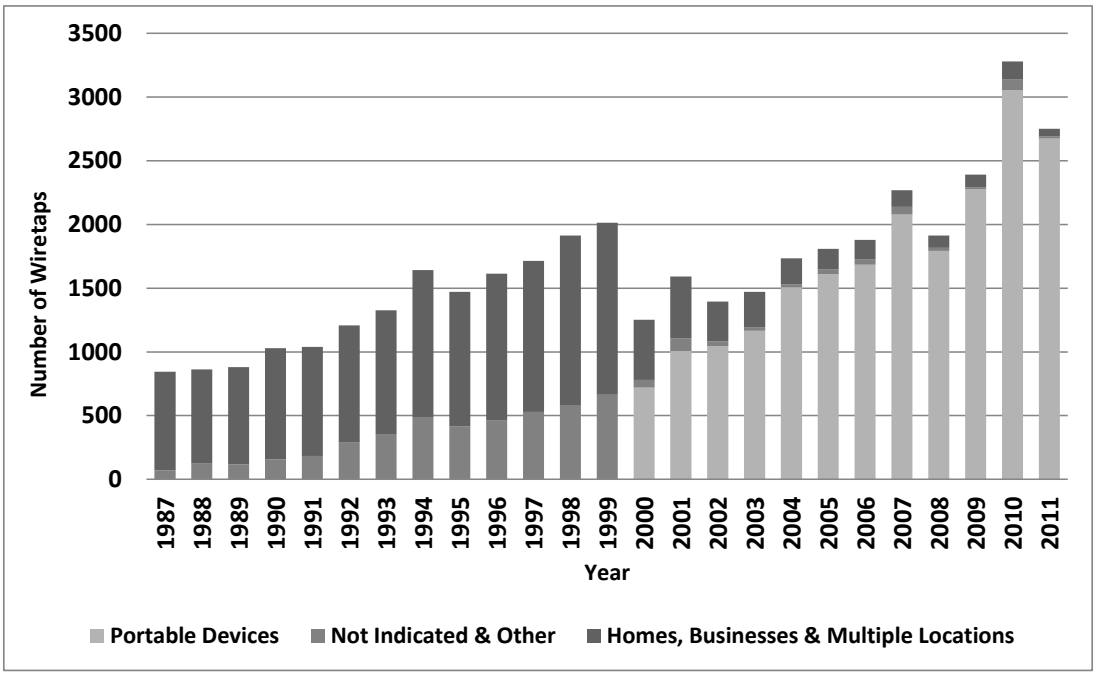

Figure 2.3: Location of Authorized Wiretaps, 1987–2011

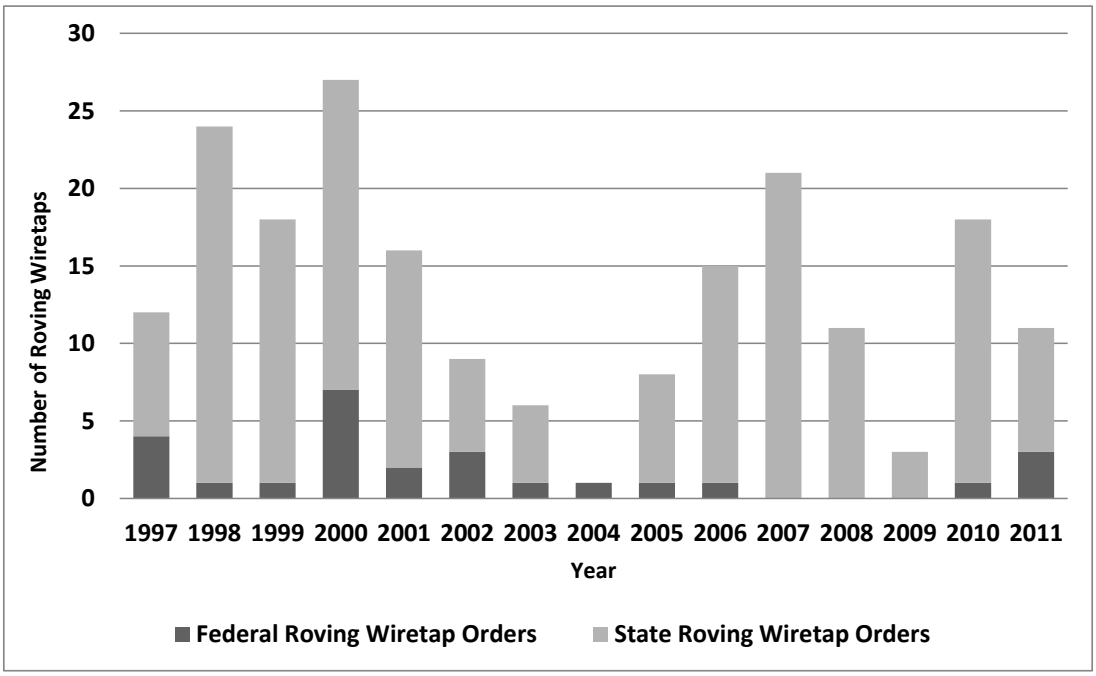

Figure 2.4: Roving Wiretap Orders Issued by Federal and State Courts, 1997–2011

Roving authority is rarely used Wiretap orders must identify the specific telephone line, connection or facility to be monitored. If, however, law enforcement agencies can demonstrate probable cause to believe that the surveillance target is actively thwarting interception — such as by using and abandoning low-cost "burner" mobile phones — courts are able to issue special *roving* intercept orders that do not need to list specific connections or facilities.[16] Although government officials often complain about drug dealers using and abandoning prepaid, anonymous mobile phones to avoid police surveillance [28, 29], the wiretap reports reveal that roving orders are rarely sought. Between 1997 and 2011, approximately 13 roving orders have been issued on average nationwide each year.

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 2011 report reveals that 95 percent federal wiretap and 81 percent of the state wiretap orders that year were sought in narcotics investigations.[17]

These numbers are not too surprising, given that the first wiretapping case in Supreme Court history, *Olmstead v. United States*, involved government efforts to investigate bootleggers. While the particular drug has changed, law enforcement communications surveillance resources still seem almost entirely dedicated to enforcing prohibitions.[18]

6 at places of business, 20 orders for multiple locations and 8 "other."

[15] A majority of traditional wire-line telephone switches still do not support modern interception technologies, in contrast to wireless switches, all of which support automated, remote interception [27].

[16] 18 U.S.C. § 2518(11)(a) and (b).

[17] The next largest categories are homicide/assault, "other," and larceny/theft/robbery each of which accounted for four percent or less of the total number of orders granted.

[18] There are several possible reasons for this. The first is that the operation of a drug trafficking organization requires ongoing, regular communication, providing law enforcement agencies with multiple opportunities to intercept and track suspects while crimes are still being committed. A second is that individuals committing drug related offenses are likely to have large amounts of money and other valuable assets gained through the sale of drugs that can be seized and kept by law enforcement agencies. As such, drug investigations are likely to pay for themselves, probably more than any other type of crime.

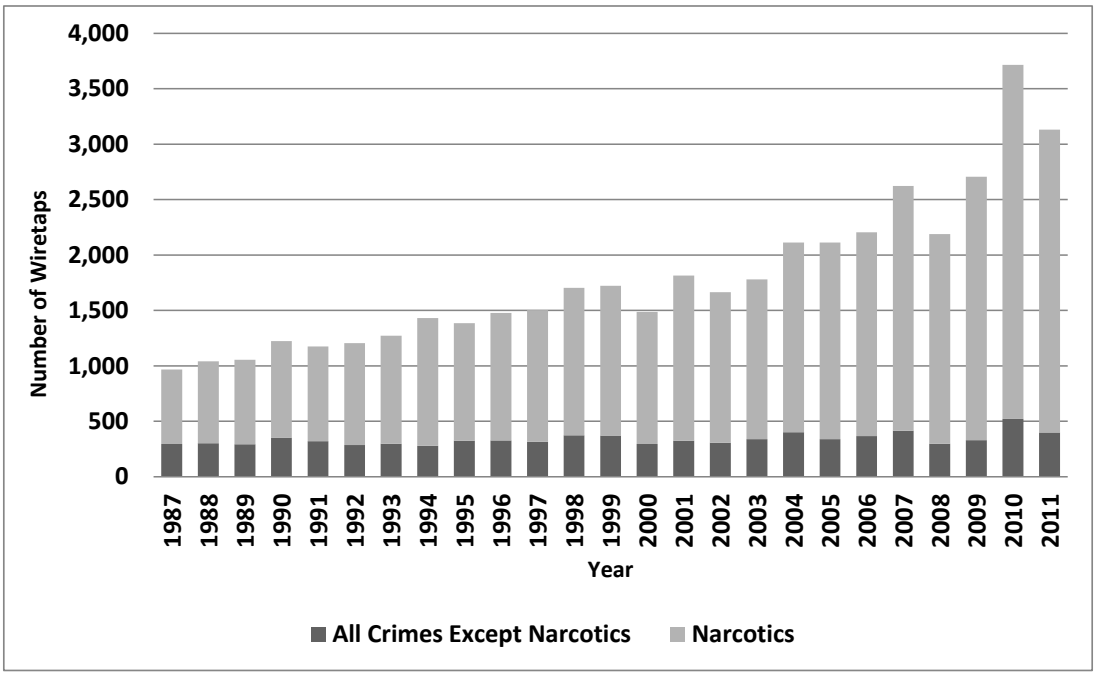

Figure 2.5: Narcotics vs. All Offenses for Which Wiretaps Were Granted, 1987–2011

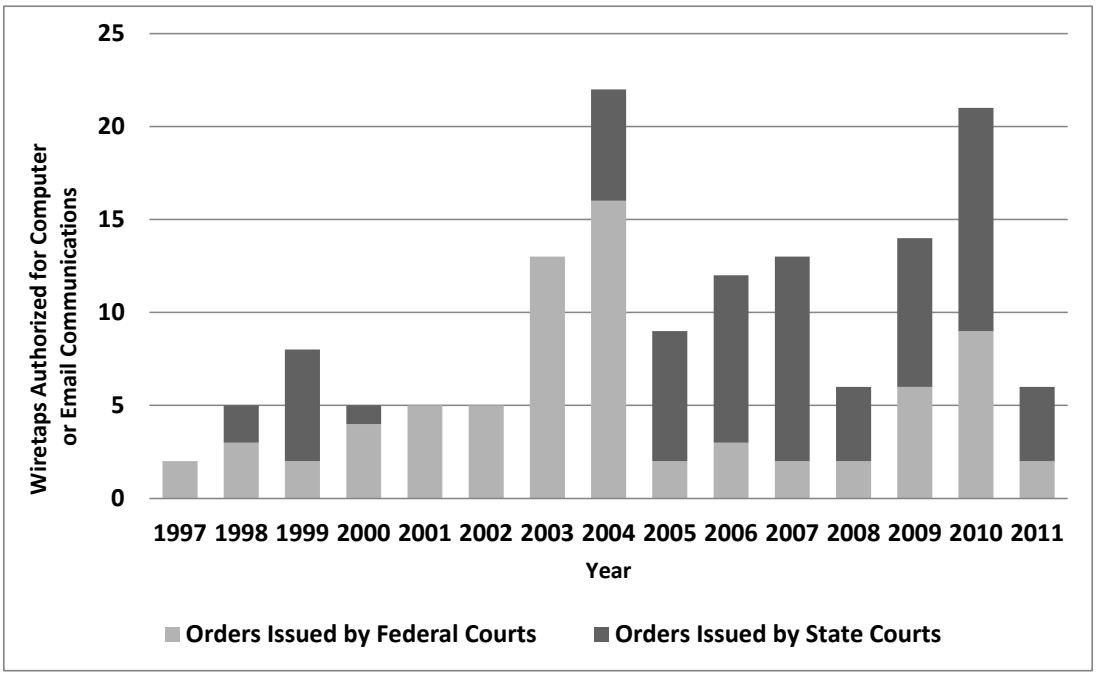

Figure 2.6: Wiretap Orders for Computers or Email Communications, 1997–2011

Wiretaps of computers and email The wiretap reports include specific categories describing the location and type of each 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 between 1997 and 2011, federal law enforcement agencies obtained just 76 of these intercept orders, while an additional 70 were issued to state law enforcement agencies.

Based upon the numbers in the annual wiretap report, it is 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,[19] and it is often easier and cheaper to do it after the fact rather than in real-time.[20]

Incidents of cryptography encountered in criminal investigations During the late 1990s, 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 [33, 34]. Responding to the fears expressed by the law enforcement community, Congress amended the existing wiretap reporting statute in 2000 to require the creation of statistics on the number of intercepts in which encryption was encountered and whether it prevented law enforcement from obtaining the contents of communications.

[19] Network communications are often retained for long periods of time, by default. For example, if the police do not wiretap a telephone call in real-time, they will not get another opportunity to obtain the communication at a later date. This is because telephone calls are typically ephemeral: after the words leave the mouths of the callers, they are gone. In contrast, if the police do not intercept an email as it is sent over the network, they can go to the surveillance target's email provider days or weeks later to obtain a copy of it.

[20] Consider that the real-time interception of an email in transit requires an interception order, but the email can be obtained from the target's email provider once it has been received with a probable cause warrant issued under Rule 41. Likewise, the cost of a real-time network intercept can range between $700 and $2400, depending on the carrier [30], while the stored emails can be obtained for approximately $25 [31, 32].

Year	State and Federal Wiretaps in Which Encryption was Encountered	Wiretaps Where Encryption Prevented Officials Obtaining the Contents of Communications
2000	22	0
2001	34	0
2002	16	0
2003	1	0
2004	2	0
2005	13	0
2006	0	0
2007	0	0
2008	2	0
2009	1	0
2010	6	0
2011	12	0

Table 2.1: Instances of Encryption Encountered During Wiretaps, 2000–2011

According to these reports, during the last decade, there have been 109 instances in which encryption was encountered during federal or state wiretaps, and *not a single instance* in which the encryption prevented law enforcement officials from obtaining the contents of the communications. Furthermore, between 2006 and 2009, the number of instances in which encryption was encountered plunged to less than 2 cases per year. These numbers strongly contradict the doomsday scenarios that law enforcement officials warned would occur due to the widespread availability of encryption technology.[21]

In 2010, as part of a high-profile lobbying campaign advocating expanded surveillance powers including encryption backdoors [35], a representative from the FBI told Jim Dempsey of the Center for Democracy and Technology 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]. Subsequent

[21] 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 or seized device. As explained earlier in this chapter, law enforcement agencies conduct very few intercepts of computers or Internet traffic, and so it is not too surprising that they rarely encounter encryption.

wiretap reports for the years 2010 and 2011 did indeed show an increase in encryption encountered by state law enforcement agencies,[22] but not by federal law enforcement agencies, who have not reported encountering encryption during an intercept since 2004.

2.1.2 Real-time interception of non-content communications records

Pen register and trap and trace orders are used by law enforcement agencies to obtain non-content communications records in real-time, such as phone numbers, *to* and *from* information associated with email messages and the IP addresses of computers to which a suspect connects.[23] With the passage of the Electronic Communications Privacy Act in 1986, Congress required that annual statistical reports on the use of this surveillance method be compiled and submitted by the Attorney General [37]. These reporting requirements were subsequently expanded in 2000.[24] Describing his reasons for expanding the reporting requirements, Senator Patrick 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" [16].

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 U.S. Courts, which after two decades of reliably producing the wiretap reports, would

[22] State law enforcement agencies encountered encryption during intercepts six times in 2010 and twelve times in 2011, a 600 percent and 1,200 percent increase, respectively, over the single instance of encryption encountered in 2009.

[23] A pen register records all outgoing communications metadata, whereas a trap and trace records all incoming communications metadata.

[24] 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.

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. Due to this restriction, the reports do not apply to surveillance conducted by other federal law enforcement agencies, such as the Secret Service, or by state and local law enforcement agencies.

The pen register reports were intended to inform both the general public as well as Congress about the use and scale of these surveillance techniques.[25] Unfortunately, the Department of Justice has repeatedly failed to submit the reports to Congress on an annual basis as it is required to by law.[26] Professor Paul Schwartz has noted that that once the reports eventually reach Congress, they "are not publicly available and generally disappear into a congressional vacuum" [38].[27] Schwartz has also observed that the reports, "fail to detail all of the information that the Pen Register Act requires to be shared with Congress" [38].[28]

[25] Describing his motivation for expanding the reporting requirements, Senator Patrick Leahy stated in 1999 that "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" [16].

[26] In 2004, the Department of Justice sent a single "document dump" to Congress, which included reports for the years 1999 through 2003 [38]. The Department of Justice did not provide Congress with any additional reports until 2009, when it submitted another document dump, this time containing the reports for the years 2004 through 2008 [39]. However, in 2010, a DOJ official told me that the Department had recently instituted policies designed to ensure that the reports would be submitted on time in the future [40].

[27] While the Administrative Office of the U.S. 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. Statistics for the years 1994 to 1998 were obtained by a staff attorney at the Electronic Privacy Information Center with contacts in Congress [41]. The Electronic Frontier Foundation obtained copies of the reports for the years 1999-2003 through a Freedom of Information Act request. DOJ took over three years to respond to that request and release the reports [42]. I obtained copies of the reports for 2004-2009 through Freedom of Information Act requests. In 2010, the Department of Justice established a policy of proactively posting copies of the pen register reports to its website [43] — a policy that DOJ has failed to uphold. In the two years since the DOJ promised that it would publish the reports to its website "annually as a mater of course whenever they become available," it failed to release any additional reports [43]. In May 2012, the ACLU filed a Freedom of Information Act lawsuit against the Department of Justice seeking copies of the pen register and trap & trace reports for 2010 and 2011 [44].

[28] 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) [45].

Analysis of existing reports As these reports do not include statistics 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.[29] Even with these significant flaws, the reports do reveal some interesting trends, such as the massive growth in the use of these metadata surveillance orders.

In 1987, the first year for which data exists, there were 1,682 pen register and 97 trap and trace orders obtained by agencies within the Department of Justice [41]. Although the numbers have fluctuated somewhat over time,[30] the number of requests has skyrocketed. By 2009, the latest year for which statistical reports are public, 12,444 pen registers and 11,091 trap and trace orders were issued. As such, this surveillance method vastly outnumbers wiretaps — in 2009, there were 18 times more pen registers than federal wiretaps.

Since 2004, the reports have included data on the use of non-content intercepts for email and network traffic. These numbers remain low: just 20 pen registers in 2004 (obtained by the Drug Enforcement Administration), eventually increasing to 258 pen registers and 50 trap and trace orders obtained by four different federal law enforcement agencies in 2009.

2.1.3 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 service provider *can*

[29] Each year, state law enforcement agencies obtain far more wiretap orders than federal agencies. (1,940 and 792 respectively in 2011). It therefore seems reasonable to assume that the number of pen register and trap and trace orders obtained by state law enforcement agencies is also higher than the number obtained by federal agencies.

[30] An interesting trend worth highlighting 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).

— 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" [46].

With the passage of the USA PATRIOT Improvement and Reauthorization Act of 2005, Congress created statistical reporting requirements for some emergency disclosures. In describing his motivation for introducing the requirement, Congressman Dan 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 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" [47].

As with the pen register 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.

Likewise, although 18 U.S.C. § 2702 permits both the disclosure of the content of communications and non-content records associated with subscribers and their communications, the reporting requirements only apply to the disclosure of communications content. It is not clear why Congress limited the reports in this way.

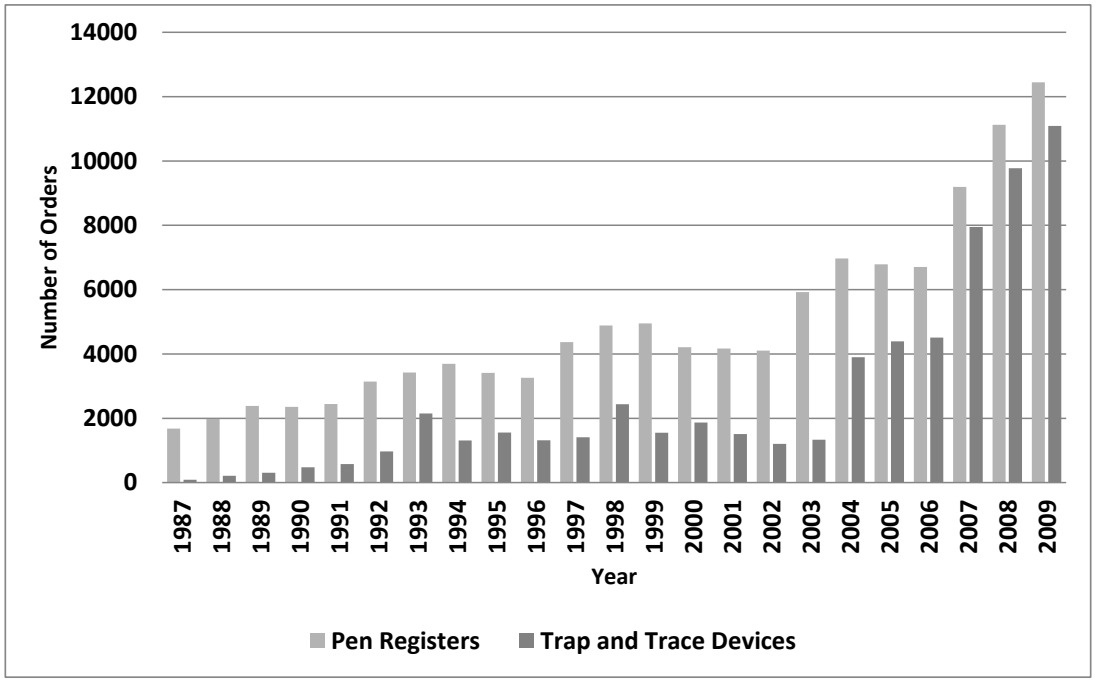

Figure 2.7: Pen Registers and Trap and Trace Orders Obtained by DOJ Agencies, 1987–2009

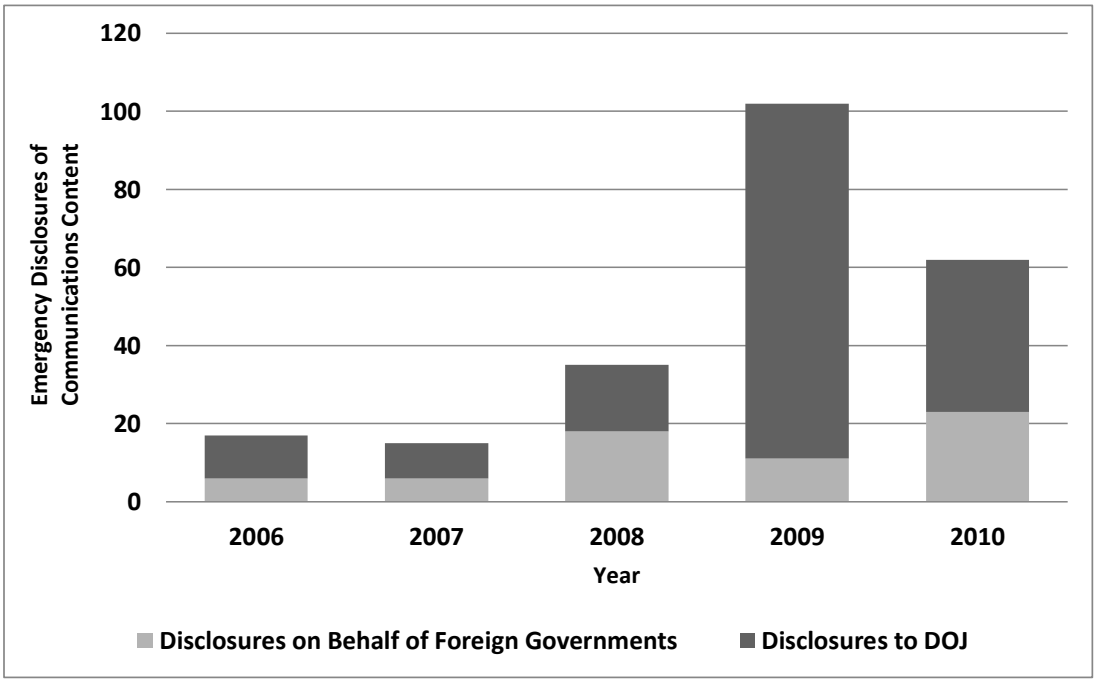

Figure 2.8: Emergency Disclosures of Communications Content, 2006–2010

Analysis of existing reports Because the reports do not document disclosures made to law enforcement agencies outside the Department of Justice, and do not include the disclosure of communications metadata and other subscriber records, the reports reveal a very limited portion of the scale of voluntary disclosures to law enforcement agencies.

Although the Department of Justice has not proactively made these reports available to the general public, I have obtained the reports for 2007–2010.[31] The most recent report reveals that in 2010, law enforcement agencies within the Department of Justice sought and obtained communications content for 39 accounts. In the same year, DOJ also sought the contents of 23 accounts on behalf of foreign governments.

While there are no comprehensive public statistics documenting the scale of emergency requests, self-reported numbers from one communications carrier reveal that there are far more requests than those that appear in the official annual report. A letter submitted by Verizon to congressional committees revealed that the company received 25,000 emergency requests during 2006 [17].[32] In contrast, the report submitted to Congress by the attorney general reveal less than 20 disclosures for that same year [48]. Even though no other service providers have released statistics for their own emergency disclosures, it is quite clear that the official reports do not adequately document the scale of this form of surveillance. In fact, they underreport these disclosures by at least three orders of magnitude.

2.2 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

[31] The reports for 2007 and 2008 were provided to me by someone with connections in Congress. I obtained the reports for 2008 through 2010 via Freedom of Information Act requests.

[32] Of these 25,000 emergency requests, just 300 requests were from federal law enforcement agencies.

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 publicly 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 [49, 50].

Requests to service providers for stored communications and subscriber records The Stored Communications Act permits law enforcement agencies to obtain stored communications and subscriber records. This includes historical call records, stored emails, instant messages, web browsing history, search engine records as well as documents stored "in the cloud."

Over the past decade, a few service providers voluntarily revealed aggregate statistics regarding the number of requests they have received from law enforcement agencies, typically in statements to journalists.[33] These disclosures were all one-time events though, making it impossible for others to observe surveillance trends. In 2010, Google started regularly publishing statistics regarding the number of requests for user data the company receives from governments around the world, broken down by country [54]. The company publishes updated statistics twice a year. In 2012, Dropbox, SpiderOak, Sonic.net, LinkedIn and Twitter followed Google's lead by publishing government request reports, which they pledged to regularly update [55, 56, 57, 58, 59].

[33] BellSouth was the first company to voluntarily disclose surveillance statistics, telling a journalist in 2003 that it received more than 32,000 subpoenas and 600 court orders per year for customer information [51]. AOL and Facebook followed suit in later years, telling journalists that the companies were receiving approximately 1000 requests per month, and somewhere between 300 and 600 requests per month, respectively [5, 52]. In response to a copyright lawsuit in 2010, Time Warner revealed that it received on average 500 requests per month for IP address records associated with its cable customers, nearly all of which came from law enforcement [53].

Surveillance of location information Law enforcement agencies also routinely compel the disclosure of geo-location information from wireless carriers [60, 61], although the legal standard required to obtain historical and real-time data is by no means settled [62]. Each wireless carrier receives thousands of requests per month, an amount that has grown "exponentially" over the past few years [63]. In order to cope with the flood of requests that they receive, many of the major wireless carriers have created automated web interfaces, through which law enforcement agents can monitor the location of surveillance targets from the comfort of their desks [64].

2.2.1 The Markey letters

In May 2012, Congressman Edward Markey wrote to nine wireless carriers, asking about their routine disclosure of customer information to law enforcement agencies. The responses from the carriers reveal that the scale of communications surveillance is far greater than previously disclosed to the public in official reports: approximately one and a half million requests from law enforcement agencies in 2011 [65].[34] More than half of these requests were subpoenas, and were therefore likely issued without judicial review.[35]

When asked by a journalist for his reaction to the number of surveillance requests, Mr. Markey confessed that he "never expected it to be this massive" [65].[36]

[34] The letters reveal that the wireless carriers received approximately 1.3 million requests in 2011. However, although T-Mobile responded to Mr. Markey, it declined to provide him with surveillance statistics. Soon after, T-Mobile revealed to a telecom industry newsletter that it received 191,000 requests from law enforcement agencies in 2011 [66]. Neustar, which did not receive a letter from Mr. Markey, voluntarily published statistics covering the four hundred smaller telecommunications companies for which it provides outsourced surveillance assistance: The company received 12,500 requests in 2011" [67].

[35] Sprint received 500,000 subpoenas in 2011 [68], while AT&T and Verizon each received 130,000 [69, 70]."

[36] Most of the carriers provided aggregate numbers to Mr. Markey, and when they did break them down, usually did so by category of legal request, not the type of data requested. For example, Sprint was the only company to provide specific statistics revealing the number of requests for subscriber geo-location it has received: nearly 200,000 requests in five years [68]. Finally, as Julian Sanchez observed, "there's no consistent way the different carriers are counting requests — and even within a single carrier, the method seems to vary by category of information" [71].

3

Mandated surveillance capabilities and assistance

> "There is a problem with the government which is that they have guns and we don't . . . We are required to follow U.S. law, and we do so, even if we don't like it. As the CEO of a public company (or a private company) there can be no other answer" [72].
>
> —ERIC SCHMIDT, CHIEF EXECUTIVE OFFICER, GOOGLE

Technology and communications companies are regularly compelled to modify their products in order to facilitate government surveillance. This compelled assistance can come in several forms: First, Congress has required that companies in particular industries build surveillance capabilities directly into their products. Examples of this include the Communications Assistance For Law Enforcement Act (CALEA) interception requirements forced on communications network providers and the E-911 geo-location requirements forced upon wireless telephone carriers. Second, where Congress has not enacted specific legislation, the courts have required firms to make surveillance enabling technical changes to products already on the market. Third, in other areas, the courts have permitted law enforcement to repurpose existing features in commercial products for surveillance.

The surveillance requirements in CALEA and E-911 are no mystery to scholars [73, 74,

75] — both were enacted through legislation, implemented via a public regulatory rule-making process and then standardized by technical bodies. In contrast, judicially mandated surveillance has received far less attention from legal scholars and technical experts. It is for this reason that this chapter will explore these later two scenarios via several case studies.

3.1 Judicially compelled surveillance assistance

Other than the CALEA and E-911 requirements forced upon certain telecommunications companies, U.S. law does not generally require that firms build surveillance capabilities into their products and services. Even so, in several instances, specific companies, on a case-by-case basis, have been forced by the courts to add backdoors to their products in order to facilitate access their subscribers' private information. This power to compel the creation of new features can be used against all companies, even those that have gone out of their way to build their products to be privacy preserving.

3.1.1 TorrentSpy

In 2006, TorrentSpy, a popular peer-to-peer filesharing search engine was taken to court by the Motion Picture Association of America (MPAA). TorrentSpy had intentionally disabled the logging of any data on its visitors, so that if compelled to, it would be unable to provide any information identifying its users. The company had also inserted clear language in its privacy policy to inform its users that it would not monitor their activity without their consent [76].

Ultimately, the MPAA convinced a federal judge to force TorrentSpy to enable logging on its servers — that is, to modify the code running on its servers in order to capture IP

address records for its visitors.[37] Demonstrating a defiant streak common amongst those in the BitTorrent community [78], TorrentSpy thumbed its nose at the judge's order, and simply blocked all U.S. visitors from accessing the site,[38] blaming an "uncertain legal climate in the US regarding user privacy and an apparent tension between US and European Union privacy laws [79]."

3.1.2 Hushmail

> "No one should be promising their customers that they will thumb their nose at a U.S. court order . . . They can promise strong encryption. They just need to figure out how they can provide us plain text." [35].
>
> —VALERIE CAPRONI, GENERAL COUNSEL, FEDERAL BUREAU OF INVESTIGATION

Since 1999, Hush Communications, a Canadian technology company, has offered consumers a free web-based encrypted email service. In contrast to the popular free webmail services provided by firms like Microsoft, Yahoo! and Google, Hushmail enables its customers to compose, transmit and receive encrypted emails that are protected using an encryption key only known to the user. With this service, it is possible to securely communicate with another Hushmail user or one of the millions of existing users of OpenPGP compatible encryption tools.

Hushmail offers two different forms of encrypted webmail. In the default mode, the user transmits her password to Hush's servers, which is then used to decrypt each email, after which the plaintext is transmitted back to the user. A more secure service uses a Java applet to download the encrypted email messages from Hush's servers each of which is then decrypted locally. This latter approach is significantly more secure, as the password

[37] The judge relied upon the fact that IP address information is available in computer memory, if just for a few seconds, as evidence that the information is "stored" and thus the company could be compelled to retain it [77].

[38] Of course, if no U.S. residents could interact with the website, then there would be no data that would need to be retained. As a result, TorrentSpy did not necessarily violate the judge's order.

never leaves the user's computer and the decrypted emails never touch Hush's servers [80].

While Hushmail's own marketing materials long promised users absolute privacy [81], a drug-related court case proved otherwise. In 2007, Hush received an order from the Supreme Court of British Columbia in response to a Mutual Legal Assistance Treaty request by the U.S. Drug Enforcement Agency. The court order requested the plain-text of three individuals' email accounts, all of whom were using the less-secure of Hushmail's two webmail products. Pursuant to the court order, Hush modified their product to capture the passwords of the three suspects, which it then used to decrypt the encrypted emails of the three surveillance targets.[39]

3.2 Build it and they will come

In addition to requiring that companies add new features to their products, the government can often compel companies to use or repurpose existing technologies and features for surveillance. Thus, companies that have deployed new products and features have unintentionally facilitated surveillance methods that were not required of their competitors, who opted not to deploy such technologies.

3.2.1 Community of interest databases

> "It is common in [surveillance orders for cellular location data] for the government to seek the location of the community of interest: that is, the location of persons with whom the target communicates" [82].
>
> —AL GIDARI

[39] While the Java-based solution would have protected Hushmail's customers against this particular form of government compelled circumvention of data encryption, it is by no means foolproof. Just as the company was compelled to modify the code that ran on its own servers, it could also be compelled to create a modified version of its Java tool capable of stealing passwords entered by users on their own computers [81].

In the late 1990s, researchers at AT&T created the Hancock programming language to enable efficient data mining of the company's telephone and Internet access records. The system was originally created to develop marketing leads and as an anti-fraud tool to target new customers who called the same numbers as previously identified fraudsters — something the original researchers referred to as "guilt by association" [83]. However, the government soon took an interest in the ability to sift through the telecom giant's vast databases.

In 2007, it was revealed that the FBI had been seeking "community of interest" or "calling circle" records from several telecommunications providers [84]. These records might include an analysis of which people the targets called most frequently, how long they generally talked and at what times of day, sudden fluctuations in activity, geographic regions that were called, and other data. A subsequent investigation by the Inspector General of the Department of Justice found the FBI had widely abused its surveillance powers, including the use of community of interest requests.[40]

Verizon also received requests to "identify a 'calling circle' for . . . telephone numbers based on a two-generation community of interest [and] provide subscriber information" [17]. However, because the company did not maintain a community of interest database, it was able to ignore that component of the requests that it received. The researchers who originally created AT&T's community of interest system likely did not plan for their tool to be used by the government to expand its surveillance dragnet. However, once AT&T had the system in place, law enforcement agents could compel its use. In contrast, Verizon effectively protected its customers' from overbroad, wholesale requests for their information by not deploying a similar system.

[40] According to the Inspector General report, "[AT&T] records show that from 2004 to 2007, [AT&T] analysts [embedded within the FBI's Telecommunications Data Collection Center] used [AT&T's] community of interest [redacted] to review records in its database for 10,070 [redacted] telephone numbers" [85].

3.2.2 In-car navigation systems

In 2003, the Ninth Circuit Court of Appeals ruled that providers of in-car GPS-enhanced navigational services can, in some situations, be forced to secretly enable microphones in a customer's car and record conversations taking place inside the vehicle.[41] These navigation systems, the most well-known of which is the OnStar service, enable drivers to press a button in their vehicles to call for help whenever they get lost or have an accident. They are typically pre-installed by car manufacturers, who also install microphones in the vehicles — permitting the driver to speak to call center workers when their assistance is needed.

The FBI took an interest in the microphones pre-installed in many luxury vehicles, and the cellular transmission capabilities of the in-car navigational systems. Specifically, FBI agents sought to covertly enable microphones without the targets' knowledge, and then use the existing cellular capabilities in the system to monitor conversations between the driver and passengers.

The Court of Appeals ruled that the FBI has the legal authority to order companies to turn their own technology against their customers. However, due to the fact that the surveillance severely limited the navigation provider's ability to deliver emergency services to its customers, the court ruled that the FBI's surveillance order was unlawful and should not have been issued by the district court in the first place.[42]

While the decision protected customer privacy in this particular case, the court left a clear path for compelled assistance with covert surveillance if doing so does not hinder a company's ability to provide service to its customers. If anything, this rather hollow victory for the privacy community was actually a win for the government.

[41] *See In re the U.S. for an Order Auth. the Roving Interception of Oral Commc'n*, 349 F.3d 1132 (9th Cir. 2003).

[42] Pointing to the *minimum of interference* language in 18 U.S.C. § 2518, the court stated that "[t]he obligation of private citizens to assist law enforcement, even if they are compensated for the immediate costs of doing so, has not extended to circumstances in which there is a complete disruption of a service they offer to a customer as part of their business."

4

The economics of modern surveillance

Cash Rules Everything Around Me
C.R.E.A.M.
Get the money
Dollar, dollar bill y'all

—WU-TANG CLAN

Although the amount of communications surveillance has significantly increased over the past half century, the amount directly performed by government agents has, as a percentage of overall surveillance, likely plunged. Surveillance has, like so many other things in recent years, been outsourced to the private sector [86].

The companies that perform most modern surveillance are not specialist firms created to address this niche business opportunity — rather, they are the very same companies that provide communications services and applications directly to consumers. Verizon, AT&T, Sprint, Comcast, Google, Microsoft and Facebook all have dedicated surveillance teams, some with more than one hundred employees, who do nothing but facilitate government surveillance of their customers [11]. For the most part, this assistance is not provided for free. Although these service providers now play a central role in the surveillance of their customers, this role is largely shrouded in secrecy — most companies go out of their way to avoid public discussion of the topic.

This chapter will focus on the economics of modern surveillance. It will analyze the impact that outsourced, carrier-provided surveillance has had on the scale of government surveillance. It will also analyze the surveillance compensation practices of many in the industry and the firms' respective attempts to keep such pricing information secret.

4.1 The changing economics of modern surveillance

> "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."
>
> —SENATE JUDICIARY COMMITTEE REPORT, OMNIBUS CRIME CONTROL AND SAFE STREETS ACT OF 1968

> "Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive."
>
> —US V. GARCIA, 474 F. 3D 994 - COURT OF APPEALS, 7TH CIRCUIT 2007

The mass adoption of digital technologies over the past decade has led to a radical shift in the government's ability to engage in large scale surveillance. Fifty years ago, if a law enforcement agency wished to monitor a suspect, it had to allocate a team of agents to engage in around the clock physical surveillance. If agents wished to monitor a target's communications, they would have to ask the post office to intercept and divert her mail, which would be steamed open, read and then sent on. Someone would also have to climb up a telephone pole or open an access panel attached to an apartment building in order to physically attach wires to the suspect's line. With the tap in place, agents would have to monitor the calls around the clock. Finally, if investigators wished to listen to conversations taking place inside her home or office, a laborious and risky "black bag job" would be necessary, in which highly skilled agents break in and covertly install microphones and remote transmitters [87].

Times have changed, as have wiretapping techniques [3]. Telecommunications companies and Internet service providers now have dedicated legal compliance departments some open twenty-four hours per day, through which law enforcement agents can obtain wiretaps, emails, text messages or real-time location information [88]. Once contacted, service providers can usually process the request and initiate a wiretap with a few keystrokes — all without the need to enter the target's home or manually connect wires in a switching center [27].

Even just a decade ago, if law enforcement agents wanted to get access to potentially incriminating evidence from the home computers of ten different suspects, investigators had to convince a judge that they had probable cause in order to obtain a search warrant for each target. The investigating agency would then send agents to raid the homes of the individuals, remove the computers, and later perform labor-intensive forensic analysis on those devices in order to get the files. Now that millions of consumers have switched to cloud based services, digital search and seizure has become far easier. Law enforcement agencies have essentially deputized the technology companies that provide online services and applications to end users, making these firms an essential component of the modern surveillance state. Thus, the private documents of ten individuals can now be obtained through a single subpoena to Google or Facebook — whose engineers will then locate the files (stored on the company's servers) and provide them to the government, often, without telling the customer first. The shift to cloud computing therefore benefits law enforcement in several ways: significantly reduced labor, no need to go before a judge or establish probable cause in order to obtain a warrant, as well as the complete elimination of physical risk to agents who might be injured killed during a raid.

4.2 Surveillance at near zero marginal cost

Modern surveillance technology is notable for the fact that a majority of the costs are infrastructure related [89]. Intelligence and law enforcement agencies must purchase data centers filled with expensive computer equipment [90], and then develop or buy special software for initiating, recording, cataloging and indexing the wiretaps [91, 27]. In order to facilitate such automated surveillance, Congress required telecommunication companies upgrade to modern digital switches with digital intercept capabilities and provided hundreds of millions of dollars to help pay for the development of such hardware [92]. However, once these up front or predictable fixed costs (such as salaries for agents and lawyers) have been paid for, modern surveillance is surprisingly cheap, if it costs anything at all.[43]

With the surveillance infrastructure in place, all that employees at the telecommunications provider need to do is to issue a couple commands from a computer terminal, at which point, a government server will begin receiving a suspect's communications data and other traffic [91]. The interception itself requires little to no direct supervision, and so it is just as easy to tap one, fifty or one hundred additional targets.

4.3 Carrier assisted surveillance can be better for privacy

> "Compensation generally equals sunshine and transparency. Currently, if service providers are not paid to implement wiretap solutions, if they are not paid to produce thousands and thousands of records, there is no audit trail. And if there is no audit trail, there is no visibility and transparency into how the money is spent, and you do not know what capabilities are actually being acquired" [6].
>
> —AL GIDARI

[43] Particularly when telecommunications companies provide the government unfettered access to their backbone networks [93], the marginal cost of an additional intercept approaches zero — as the equipment, bandwidth and agent labor must be paid for no matter how many individuals are monitored.

Companies receiving surveillance assistance requests often play two, conflicting roles: they facilitate surveillance of their customers yet are often the only gatekeeper capable of resisting unreasonable or illegal demands. Many firms frequently push back against, and sometimes refuse to comply with surveillance orders that they believe violate the law [94, 95]. In some cases, this might be motivated by a corporate commitment to customer privacy, and in others, a desire to avoid the legal consequences of complying with an invalid request, including civil liability, as well as public criticism from civil liberties groups and the media [96, 97].

Federal wiretapping laws include civil liability for companies that improperly share customer information with third parties, such as the government. The possibility of fines and costly lawsuits gives telecommunication companies some incentive to make sure that the law is being followed.[44] Thus, when wiretaps can be performed without any involvement of the telecommunication providers, consumers are robbed of this crucial additional layer of risk-avoidance motivated oversight, and must rely upon law enforcement and intelligence agencies to not abuse their access.

When communications providers play a role in performing surveillance and, more importantly, charge for their services, subscribers benefit through the paper trail that is left behind [6]. That is, if the government is billed for each wiretap it requests, an invoice will be generated detailing the date that tap began, ended, the number of lines tapped, as well as the cost of this service. At least two copies of this will be generated, one kept by the carrier and another sent to the investigating agency. This paper trail provides a wealth of data for researchers and activists, who can often obtain the invoices through Freedom of Information Act requests [100, 101, 64, 31].

Consumers using service providers that charge on a per-transaction basis for surveillance assistance also receive some privacy benefit from resource scarcity. That is, given a

[44] Companies and their allies in the government also have an incentive to lobby for immunity from this liability [98, 99].

fixed budget and an almost endless number of possible surveillance targets, government agents are forced to prioritize their snooping [89] and avoid fishing expeditions.

Even though law enforcement agencies frequently complain about the prices they are charged by service providers [89], they are surely better off than in past decades, before digital telephone switches and cloud computing. Paying an Internet provider $2,500 for a wiretap might be unpleasant, but it is still far cheaper than sending a team of agents out to monitor a home or trail a suspect. It is also much safer.

4.4 Charging for surveillance assistance

> "When I can follow the money, I know how much of something is being consumed - how many wiretaps, how many pen registers, how many customer records. Couple that with reporting, and at least you have the opportunity to look at and know about what is going on. Because right now, you do not know" [6].
>
> —AL GIDARI

Federal law enables law enforcement and intelligence agencies to compel companies to disclose their customers' data to the government. However, the law also permits these firms to charge for this service, something that many, but not all, companies choose to do.[45] As such, most major service providers have a formal policy, often in writing, documenting the fees they charge for their assistance. However, only two companies have voluntarily published their surveillance price lists [102] — the rest consider the information to be highly confidential, and have in some cases vigorously resisted attempts to reveal it.

[45] Providers can seek compensation for many forms of surveillance assistance. For example, 18 U.S.C. § 2706(a) generally obligates government entities "obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704" to pay the service provider "a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information." However, providers are prohibited by 18 U.S.C. § 2706(c) from recovering the cost of producing phone records. It is also unclear if providers who insist on a Rule 41 order before delivering geo-location information can seek compensation [82].

Although often secret, surveillance pricing information can serve as a useful metric for evaluating service providers' willingness to facilitate surveillance of their customers. This is because the cost of surveillance assistance can have a significant impact on the extent and frequency of law enforcement requests. By analyzing law enforcement manuals and price lists for various providers that have been leaked, unintentionally placed online, or disclosed to Congress, it is possible to observe several interesting trends. Most interesting of all, are the firms who choose not to charge.

4.4.1 Current surveillance compensation policies

Many telecommunications carriers and Internet service providers seek and receive payment from government agencies for the surveillance services they provide,[46] a practice permitted by law. However, most firms voluntarily waive the fees for certain types of investigations, such as cases involving children at risk,[47] while others never charge for customer data. Such surveillance pricing decisions can have a major impact on the volume of government requests for data and on the breadth of data sought in each request [82].

A small subset of companies never seek compensation, regardless of the type of crime being investigated. That is, regardless of if the request comes from local, state or federal law enforcement, or if the crime under investigation is a murder, terrorism, drug trafficking, or corporate fraud — these technology firms have opted to provide their customers'

[46] However, just because a service provider sends the government an invoice for surveillance services does not automatically mean that the government will pay for the services rendered. Some agencies, such as those in the State of California, may conclude that they are not required to pay [103], while other agencies may simply be late in paying their bills [104].

[47] There appears to be an industry-wide norm of not seeking compensation for surveillance and data disclosures associated with missing children or child exploitation investigations. Although companies are not required by law to waive their fees, these good corporate citizens likely opted to do so recognizing that child exploitation is an emotion-fueled rhetorical bomb in the already complex debate over surveillance and data retention. Simply put, no company wants to be accused of doing anything to frustrate or profit from a child exploitation investigation.

data to the government for free. In 2010, Hemanshu Nigam, the chief security officer of MySpace confirmed that the company did not charge for the "thousands" of requests it received each year from the government [105]. Similarly, reliable sources have confirmed that Facebook does not charge the government for surveillance assistance and Microsoft did not start charging until 2012.[48]

Of the companies that do charge, costs tend to vary based on the type of user data sought and whether or not it is requested in real-time. The cost of stored email records from Google or Yahoo can be as cheap as $25 [31, 32], basic subscriber information from wireless carrier Cricket is just $5 per user [30], while Sprint charges $30 per month, per surveilled subscriber for real-time geo-location data [64]. In contrast, the fees charged by the major wireless phone companies for real-time interception of communications content range between $700 to $2400 per 30 day wiretap, depending on the carrier [30].

The decision to charge or not charge the government can have a major impact on user privacy, as telecommunications lawyer Al Gidari revealed in testimony before Congress in 2010:

> "When records are 'free' [to the government] such as with phone records, law enforcement over-consumes with abandon. Pen register print outs, for example, are served daily on carriers without regard to whether the prior day's output sought the same records. Phone record subpoenas often cover years rather than shorter, more relevant time periods. But when service providers charge for extracting data, such as log file searches, law enforcement requests are more tailored" [82].

[48] A well-informed source at Facebook told me that the company has a policy of not charging for government assistance, although its online law enforcement manual states that the company "may seek reimbursement for costs" [106]. Likewise, according to a source within Microsoft, the company had long provided user data to law enforcement agencies at no cost. After several years of pleading with lawyers at Microsoft to charge the government, I was informed in June 2012 that the company had recently established a policy of seeking compensation for surveillance assistance, and that the first invoices would be sent out in July 2012.

4.4.2 Publishing surveillance prices

Although many service providers charge the government for access to their customers' data, few will voluntarily publish the fees that they charge. Cox Communications and Sonic.net are the only telecommunications providers that publish their surveillance prices on their websites [102, 107]. The prices charged by several other companies have come to light over the past few years, albeit often against the wishes of many of the respective firms.

Many law enforcement handbooks have been leaked to the Internet, including documents detailing the surveillance prices charged by Yahoo!, Comcast, Sprint, Verizon and AT&T [108, 109]. No similar document for Google has surfaced.[49] However, an invoice sent by the company to the U.S. Marshals Service confirms that Google charges for surveillance assistance [31].

In September 2009, I filed FOIA requests with several government agencies for copies of ISP surveillance price lists. Verizon's surveillance price list was one of several documents in the possession of the U.S. Marshals that were determined to be responsive to my request. When given the opportunity to object to the disclosure of its price list, Verizon argued that:

> "[W]e do not want the general public to have access to these pricing schedules. First, such information may confuse our customers ...Other customers may, upon seeing the availability of certain services to law enforcement (such as wiretapping, for instance), become unnecessarily afraid that their lines have been tapped or call Verizon to ask if their lines are tapped (a question we cannot answer)" [110].

[49] I have been told by several sources that Google does not have a law enforcement handbook.

Responding to the same FOIA request, Yahoo!'s outside counsel was even more direct, stating that:

> "[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" [50].

When copies of Yahoo's and Microsoft's law enforcement guides surfaced on the Internet whistleblower site *cryptome.org* in December 2009 and February 2010, law firms retained by both companies sent Digital Millennium Copyright Act complaints in an attempt to force the leaked documents offline. While Yahoo's complaint was entirely unsuccessful, Microsoft was able to convince cryptome's domain registrar to temporarily suspend the site's domain name. Both companies' legal efforts quickly confirmed the *Streisand Effect* [111], as the copyright complaints led to significant media attention as well as worldwide mirroring of the censored documents [32, 112].

Part II

The Companies

"Electronic surveillance for law enforcement and intelligence purposes depends in great part on the cooperation of the private companies that operate the Nation's telecommunication system" [113].

—SENATE SELECT COMMITTEE ON INTELLIGENCE REPORT,
FISA AMENDMENTS ACT OF 2007

"[Service providers] have, last time I looked, no entry in any government directory; they are not an agent of any law enforcement agency; they do not work for or report to the Federal Bureau of Investigation; and yet, you would never know that by the way law enforcement orders them around and expects blind obedience. Likewise, they are not the vanguard of privacy for their users or non-customer privacy advocates. They are neither formed nor organized for purposes of protecting user privacy, and in most cases, the law does not require it" [6].

—AL GIDARI

5

Companies differ on privacy technologies

Service providers are regularly compelled to deliver their customers' data to the government, and in some cases, are required by law to proactively retain and be able to provide certain types of data upon demand.[50] In spite of this, most technology companies in the United States are largely free to design their products any way they wish. In particular, they may include strong, privacy enhancing technologies, even if doing so might limit the effectiveness of law enforcement and intelligence agencies' lawful surveillance efforts.

This chapter will explore several ways that companies' engineering design decisions and data storage policies differ, and analyze the impact that such decisions have on their customers' privacy. Although most service providers do not advertise or compete on the ways in which they protect their customers' private data from the government, the differences are not trivial.

5.1 Leaking IP addresses in e-mail headers

Several of the large, free webmail providers intentionally leak their customers' IP addresses to the recipients of email messages. Although this form of data leakage is not

[50] For example, 47 C.F.R. § 42.6 requires carriers that offer or bill toll telephone service to "retain for a period of 18 months such records as are necessary to provide the following billing information about telephone toll calls: the name, address, and telephone number of the caller, telephone number called, date, time and length of the call."

required by any technical standard or law,[51] it can negatively impact webmail subscribers, who can potentially be identified and located by government agents using the leaked IP addresses.

When a subscriber of Microsoft's Hotmail or Yahoo! Mail sends an email message to another person, both companies insert their user's current IP address into a header sent along with the outgoing email message [114].[52] In contrast, Google generally shields the IP addresses of its webmail subscribers. A statement on the company's website confirm that privacy is a primary factor motivating this decision:

> "IP addresses can be considered sensitive information. As such, Gmail may hide sender IP address information from outgoing mail headers in some circumstances" [115].[53]

Intentionally leaking a user's IP addresses to the recipients of emails can negatively impact the subscriber's privacy. In contrast, this practice reduces the workload for service providers — who receive fewer law enforcement requests — and for the investigating law enforcement agencies.[54]

For example, in the event that a Yahoo! or Hotmail account is used to send an email message that is obtained by a U.S. law enforcement agency, the investigators will not need to send Yahoo! or Microsoft a subpoena to learn the IP address of the computer that sent

[51] It may, however, make it easier to prevent the use of these free webmail services to send spam.

[52] While this header is typically not displayed to recipients by most email clients, technically savvy users such as forensic experts working for the government can easily view the full header accompanying an email message to determine the originating IP address.

[53] Google has not publicly confirmed the specific circumstances in which the company shields or leaks IP address information. However, anecdotal reports from users reveal that the company leaks the IP addresses of consumers who use third party email clients to send mail through Google's SMTP servers. Some users, particularly those using Google Apps with custom domains rather than Gmail, also report leakage of their IP address via a X-Originating-IP header even when using the webmail interface.

[54] For foreign government agents, this is not just a time-saver, but a source of data that would otherwise not be available, due to the fact that many western service providers refuse to comply with requests for user data from certain countries.

the message. Instead, the investigators can simply examine the header and then go directly to the broadband Internet service provider responsible for that IP address in order to identify the sender. Thus, by providing this IP address information in the header of every outgoing email, Yahoo! and Microsoft significantly reduce the need for law enforcement agents to contact them to get this form of user data.

If Yahoo! or Microsoft did not proactively disclose the IP address information in the email headers, law enforcement investigators would have to obtain a subpoena, serve it on the companies, and then wait days or weeks for the companies to provide the data. In addition to the delay, this extra step would give the service providers the opportunity to notify their customers about the subpoena, or force the police to obtain a gag order from a judge under 18 U.S.C. § 2705(b).

By forcing law enforcement agencies to contact webmail providers in order to determine a suspect's IP address, webmail providers can insert themselves as choke points in the surveillance of their customers, carefully evaluating each request for information, and rejecting those that do not meet the appropriate standard or come from a foreign government that the providers have no legal obligation to assist. For example, many U.S. based service provider regularly refuse to comply with requests from state security officials working for authoritarian foreign governments with a documented history of violating human rights,[55] thus effectively protecting the privacy of their foreign customers. In such situations, this minor speed bump becomes a highly effective privacy shield.[56]

Consider a scenario in which a pro-democracy activist in Vietnam, Zimbabwe or another foreign country with an oppressive government is using her U.S. based webmail provider to communicate. Should state security officials in her country obtain one of the

[55] At least when the companies do not have assets or employees in the country.

[56] Twitter's transparency report reveals that the company refuses to comply with all of the government requests for user data it has received from sixteen different countries [59]. Google is more helpful — there are just three countries it refuses to assist — presumably because it has staff in far more countries than Twitter [54].

email messages sent by the activist, her choice of webmail provider will significantly impact the authorities' ability to determine her identity. If the activist uses Google's Gmail service, her IP address will likely be shielded and therefore, the only way for the government to learn her IP address will be to contact Google and ask for the information, a request that the company is likely to reject. In contrast, if the activist uses Microsoft Hotmail or Yahoo! Mail, the investigators will be able to easily locate her IP address in the header of the received email, and then go directly to her domestic Internet service provider in order to identify her. Even if Yahoo! or Microsoft refuse to cooperate with the authorities in Zimbabwe or Myanmar, such policies will often do little to protect the identity of their webmail customers in those countries.

By automatically including their subscribers' IP addresses in the headers of outbound email messages, Microsoft and Yahoo! have passed up the opportunity to protect their customers from unreasonable or illegal law enforcement investigations. In exchange, the companies have also reduced the administrative labor costs associated with responding to many IP record requests from government agencies.[57]

5.2 Proactive searches for child pornography

Internet service providers are obligated by 18 U.S.C. § 2258A to immediately notify the authorities when they detect or otherwise learn about the presence of child pornography on their servers. In order to comply with the law, most large Internet companies, particularly those that host user generated images and videos, review content that has been

[57] Starting in 2005, Yahoo! was the subject of a high-profile human rights scandal relating to the company's disclosure to the Chinese government of email account records of several journalists [116]. By continuing to leak its customers' IP addresses, Yahoo! has struck a balance of sorts: China and other authoritarian governments continue to passively receive data that can enable the efficient investigation of dissidents, without Yahoo! having to get its hands dirty by responding to user data requests from those governments. Although Yahoo! certainly learned a lesson from its role in the jailing of Chinese journalists — during a congressional hearing focused on the incident, Yahoo's CEO Jerry Yang was publicly lambasted by the committee chairman as moral pygmy — it remains unclear if Yahoo! learned the *right* lesson.

flagged by their users or other third parties [117]. The law does not, however, require that service providers proactively seek out such materials by automatically analyzing their customers' communications. Nevertheless, several companies do so anyway.

In 2002, AOL voluntarily developed and began using a proprietary Image Detection and Filtering Program, which calculates a cryptographic hash of each file attached to email messages sent or received by its customers.[58] Each of these is then compared against a database of hashes for images that AOL has previously identified as child pornography. In the event that two hashes match, the company notifies the National Center for Missing and Exploited Center (NCMEC), as required by law.

Child pornography is a complex emotional issue that plagues the debate over online privacy. No company wishes to be seen as fighting for the rights of child pornographers, and as such, it is extremely difficult to engage in a reasonable public discussion about the extent to which consumers' privacy can and should be sacrificed in order to assist the government in its attempts to detect and prosecute these crimes. Furthermore, while many service providers and legal experts might have reservations about the tactics used by government investigators, prosecutors, and the quasi-government NCMEC, few will publicly voice their complaints [118].

AOL's decision to proactively scan its customers' email attachments for child pornography negatively impacts their privacy, and more importantly, the impact of this system extends far beyond the company's desire to assist in the discovery of this particularly horrible form of illegal content. The reason for this is that once the technical infrastructure for automatically intercepting and examining user communications has been designed and deployed, service providers are not in a position to limit the extent to which they can be compelled to use it [119]. Thus, AOL's automatic email attachment analysis system

[58] *See United States v. Richardson*, 607 F.3d 357, 363 (4th Cir. 2010).

could also be used to determine if its customers are transmitting bomb making instructions, copyrighted images, songs and books, seditious newsletters, or religious texts. Such expanded surveillance can be performed, quite easily, if the government provides AOL with a list of additional hashes to add to the company's database and then forces the company to detect the transmission of those other types of prohibited content.[59]

AOL's engineers and legal team likely had noble intentions in developing the company's email attachment scanning system. It is also quite possible that the vast majority of AOL's customers might even approve of the scanning and the associated intrusion into their communications privacy if told about it. However, the service may eventually be used to detect and identify other forms of content that many of AOL's customers are more likely to believe are legitimately private.

While AOL was the first U.S. service provider to embrace this practice, it is not longer the only company to do so. In June 2010, several large social networks, including Facebook and MySpace announced that they too would be scanning their customers' uploaded images against a database of child pornography hash signatures provided by the New York Attorney General [120].[60]

5.3 Encryption

Encryption technologies have been readily available to the general public for more than a two decades, are now included in all modern operating systems and web browsers, and

[59] There is, of course, no need for the government to tell AOL what kind of content it is looking for, if the company is simply provided with a set of hashes.

[60] Facebook has also voluntarily deployed an automated system that scans the contents of posted messages and chats between users for keywords associated with criminal behavior, which are then manually reviewed by Facebook employees [121].

as such are widely used for many web-based products and services. For example, encryption is routinely used to protect sensitive data (such as credit card numbers) in transit between a shopper's computer and e-commerce websites. Increasingly, some companies are also encrypting their customers' data in storage, so that no one other than the subscriber can access the data, including the service provider itself.

Existing federal law protects the rights of telecommunications carriers and technology firms to add encryption capabilities to their products.[61] If a company does not have access to the encryption key, or other "information necessary to decrypt the communication," it has no legal obligation to decrypt its customers' data, or otherwise provide the government with the ability to decrypt encrypted communications. However, if the company does have a copy of (or access to) the decryption key, it can be compelled to decrypt its customers' data.

5.3.1 Transport encryption

Encryption technology can shield consumers from several privacy threats when it is used to protect their private information in transit. These threats include criminals intercepting data and hijacking users' accounts; service providers using deep packet inspection technology to analyze users' communication data in order to deliver behavioral advertising [123]; and passive, network-based surveillance by government agencies.[62]

[61] The legislative history for CALEA notes that "telecommunications carriers have no responsibility to decrypt encrypted communications that are the subject of court-ordered wiretaps, unless the carrier provided the encryption and can decrypt it ...Nothing in [47 U.S.C § 1002 (b)(3)] would prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access ...Nothing in [CALEA] is intended to limit or otherwise prevent the use of any type of encryption within the United States. Nor does the Committee intend [CALEA] to be in any way a precursor to any kind of ban or limitation on encryption technology. To the contrary, [CALEA] protects the right to use encryption" [122].

[62] Transport encryption doesn't totally prevent government surveillance. Rather, it forces the authorities to go directly to the company storing the data, rather than being able to passively intercept it in transit.

Although the banking and finance industries have long used HTTPS transport encryption to enable their customers to conduct secure transactions at home, most major social networks, email and cloud computing services remain, by default, insecure. This is because these services do not use encryption to protect user data in transit [124]. However in recent years, a few companies such as Google and Twitter have started to encrypt data in transit by default.

When Google launched its Gmail email service in 2004, it offered HTTPS transport encryption as an option, although not enabled by default. Likewise, when the company later introduced its Docs, Spreadsheets and Calendar products, they too could be accessed via HTTPS, but again, not by default. As recently as 2008, the company argued that the decision to use encryption should be a "choice left up to" users [125].[63]

In 2009, 38 industry and academic experts from the fields of computer security, privacy and law wrote an open letter to Google's Chief Executive Officer to chastise the company for its lack of default transport encryption [124]. Seven months later, the company enabled encryption by default for its Gmail service,[64] and approximately six months after that, also enabled encryption for its Docs, Spreadsheets and Calendar services too [128]. Similarly, in 2010, the company began to offer encrypted search [129], which it later turned on by default for signed in users, making it the first major search engine to do so [130].[65]

[63] Google claimed in 2008 that HTTPS "can make your mail slower. Your computer has to do extra work to decrypt all that data, and encrypted data doesn't travel across the internet as efficiently as unencrypted data" [125]. However, soon after the company enabled HTTPS by default for Gmail in 2010, Adam Langley, one of the company's engineers revealed that "we had to deploy no additional machines and no special hardware. On our production frontend machines, SSL/TLS accounts for less than 1% of the CPU load, less than 10KB of memory per connection and less than 2% of network overhead ... SSL/TLS is not computationally expensive any more" [126].

[64] The company announced the switch to HTTPS the same day that it revealed that its systems had been penetrated by attackers in China [127].

[65] Mozilla subsequently made Google's HTTPS search service the default search engine for all Firefox users, regardless of whether or not they are signed into a Google service [131].

Widely available tools have been available for several years that automate the cookie-stealing attacks that can be used to hijack non HTTPS protected sessions [132, 133]. However, these tools were difficult to use, often requiring advanced technical skills. In 2010, a security researcher released Firesheep, a plugin for the Firefox browser that made session hijacking easy to perform, and thus accessible to the average user [134]. The tool was downloaded more than a million times in the first month after its release and even inspired Senator Charles Schumer to write to several major cloud computing companies to ask them to enable HTTPS by default [135].

Less than one year after FTC Commissioner Pamela Jones Harbour called on cloud computing companies to deploy HTTPS by default [136] and less than six months after the release of Firesheep, Microsoft, Facebook and Twitter all began to HTTPS protection on an opt-in basis, with Twitter eventually turning it on by default [137, 138, 139, 140]. Unfortunately, Microsoft and Facebook continue to expose most of their customers to the threat of account hijacking — requiring their users to seek out and enable obscure configuration settings in order to protect themselves against account hijacking. Consumers who use Yahoo! Mail are even worse off; in contrast to the opt-in security offered by Microsoft and Facebook, Yahoo! does not offer HTTPS at all.[66] The only way for Yahoo!'s customers to protect themselves from account hijacking risks, it seems, is to switch to another email provider.

5.3.2 Storage encryption

Cloud-based services do not have to expose their customers to the risk of government seizure by storing their data in unencrypted form. Consider, for example, the Firefox Sync

[66] Yahoo uses HTTPS to transmit the username and password during the initial account login, but all subsequent transactions occur over an unencrypted HTTP connection.

feature in the Firefox web browser [141]. This feature enables users to keep their bookmarks, browsing history, passwords, and cookie synchronized across multiple devices. Although the data is stored on servers run by Mozilla, it is encrypted with a key only known to the user.[67] In the event that the government compels Mozilla to share its users' data, the only information that the company can deliver will be encrypted.[68]

Mozilla is not the only company to use encryption to securely store its customers' data in the cloud. Over the past several years, several firms have started to offer encrypted cloud-based backup solutions — enabling consumers to automatically store their personal documents and other important files online using a password that only they know.[69] Unfortunately, many of the most popular online backup services, such as those provided by Dropbox and Apple do not use encryption keys only known to the user.[70] As a result, these companies can, and are routinely forced to, disclose to the government the data users have uploaded.[71]

Similarly, the major online communications services such as Google and Facebook have yet to add any form of truly secure storage encryption to their popular cloud based services. One reason for this may be that these services are largely supported by targeted

[67] Mozilla, the organization that makes Firefox, built privacy into the product at the design stages, stating that a key design principle for Firefox Sync is that "users own their data, and have complete control over its use. Users need to explicitly enable third parties to access their data" [142].

[68] Government agencies can of course attempt to use brute force attacks to decrypt the data. However, this threat also exists even if when encrypted data is stored on the user's own computer.

[69] One online backup service, SpiderOak, describes itself as a "zero knowledge backup provider," stating that "we do not know anything about the data that you store on SpiderOak not even your folder or filenames. On the server we only see sequentially numbered containers of encrypted data" [143]. Another company, Wuala, tells its customers that "all files are directly encrypted on your desktop. Your password never leaves your computer. Not even we as the provider can access your files or your password" [144]. A third service, Tarsnap, has a similar system design, and describes its product as "online backups for the truly paranoid" [145].

[70] One of the factors influencing this decision appears to be the tradeoff between security and usability. Both companies have optimized their products for the common scenario in which users forget their passwords. In contrast, when a user of SpiderOak or Tarsnap forgets their password, they lose access to their data.

[71] On March 29, 2012, I received an on-the-record statement from an Apple spokesperson confirming that the company has access to the encryption key used to encrypt files stored with the company's iCloud backup service. Dropbox has publicly confirmed that it has access to its users' data and that it receives requests for that data from law enforcement agencies [146].

advertising, a business model that depends upon the ability to mine the contents of users' communications and other private data [147]. As it is exceedingly difficult to monetize a dataset that one cannot look at [148], the use of encryption directly conflicts with their existing business model.[72]

5.4 Data retention

> "[T]he reason we keep [search engine data] for any length of time is one, we actually need it to make our algorithms better but more importantly, there is a legitimate case of the government, or particularly, the police function or so forth, wanting, with a federal subpoena and so forth — being able to get access to that information" [149].
>
> —ERIC SCHMIDT, CHIEF EXECUTIVE OFFICER, GOOGLE

> "[Anonymized search] . . . can become a haven for child predators. We want to make sure users have control and choices, but at the same time, we want to provide a security balance" [150].
>
> —PETER CULLEN, CHIEF PRIVACY STRATEGIST, MICROSOFT

The decision to not retain or to promptly delete data is often one of the most effective ways a company can protect its customers' privacy.[73] Quite simply, if user data is not retained, there will be nothing to give law enforcement agencies if they later request it [151]. Unfortunately for users and their privacy, zero data retention periods are the exception to the rule, while lengthy, often indefinite data retention policies are far more common.

Many service providers have formal data retention policies that detail the length of time before which they will delete customer records, communications, logs, and other data.

[72] If Google does eventually offer encrypted cloud based storage, it will likely be for enterprise customers first. Google does not need to monetize their data, as these businesses pay for the Google services they use.

[73] While the decision to retain or not retain data can have a massive impact on user privacy [151], the decision over how long to keep data has far less impact. This is because most law enforcement requests for user data appear to be for data that is relatively recent. Thus, the difference between a six or twelve month retention policy is unlikely to impact most law enforcement requests [152].

However, outside of the search engine market where pressure from European regulators has led to companies revealing their policies — and in some cases, shorten their retention periods) [153] — few other firms publish their own data retention policies.

The widespread lack of public information about data retention policies is a substantial barrier for consumers wishing to evaluate potential service providers on their respective privacy merits. Furthermore, there are considerable differences among providers, which means that the decision to pick a particular company can have a major impact on a user's privacy.

A great example of this can be found in the wireless telephone market. Sprint Nextel assigns each Internet-connected wireless handset a static IP address, and logs the allocated addresses for 24 months [12]. The company also retains a record of the URL of each webpage viewed by many of its customers. Likewise, Verizon Wireless retains logs of the IP addresses issued to customers for one year, and also logs of the IP addresses of the websites visited by subscribers for one month [109].

In contrast, both T-Mobile and Cricket Communications use a Network Address Translation (NAT) based infrastructure, in which all customers from a region appear to use one of a handful of IP addresses [12]. The companies do not assign unique IP addresses to their customers, nor are they able to reveal after the fact which particular customer was responsible for traffic originating from their network.[74]

As a result of these policies, a Sprint Nextel or Verizon customer that posts an anonymous, critical comment on a blog or engages in copyright infringement can be later identified, sued or prosecuted. In contrast, customers of T-Mobile and Cricket can currently

[74]One factor that likely motivated the use of NAT by these two carriers is the global shortage of Internet Protocol Version 4 (IPv4) addresses [154]. In 2012, T-Mobile enabled IPv6 nationwide on its wireless network, albeit on an opt-in basis for a few smartphone models [155]. The eventual company-wide migration to IPv6 will likely eliminate the need for NAT, which will also neutralize the privacy protections currently enjoyed by T-Mobile's customers.

engage in a variety of online activities with less risk of later identification.[75]

While most companies are not willing to disclose their data retention periods to their customers, privacy advocates or researchers, they freely provide this information to the law enforcement community. Most Internet and telecommunications providers have created law enforcement handbooks, which list surveillance prices, include sample subpoenas and search warrant applications, and also detail the kinds of data that each firm retains, and for how long. Although these documents are typically not available to the public,[76] many have, over the past few years, leaked onto Internet or been obtained by privacy advocates through Freedom of Information Act requests. The disclosure of these law enforcement handbooks has enabled, for the first time, some degree of transparency with regard to companies' actual privacy practices.[77]

5.4.1 Data retention creep

One major problem stemming from the industry-wide norm of secrecy regarding data retention policies is that consumers are not told when the data retention periods change. Worse, other than in the case of the search engines (who are under regulatory pressure in Europe to keep less data), most data retention periods tend to increase over time.

Over a one or two year period, several major wireless carriers extended the retention period for historical cell site location information. Retention periods of six months to one year for cell site data are now common across the industry [161], a significant increase

[75] In order to enable the identification by law enforcement agencies of users with ISPs that have deployed NAT, websites and service providers are increasingly retaining port numbers in addition to IP addresses [156, 154]. In 2011, engineers from Juniper Networks, Yahoo, Facebook and AT&T jointly published a best-practices Request for Comments, which recommends that anyone operating a web server record the source port number of inbound connections "to support abuse mitigation or public safety requests" [157].

[76] Cox, Twitter, Facebook, Dropbox, Sonic.net, and LinkedIn are exceptions to this norm, however the latter four companies published their law enforcement guidelines online for the first time in 2012 [102, 158, 106, 159, 107, 160].

[77] As most companies do not publish their law enforcement guidelines, the documents that have leaked provide a single snapshot of the policies that existed at a particular moment.

over the 30 days or less that the data was retained as recently as 2008 [61]. The move to increase data retention seems to have been a voluntary decision on the part of the carriers. However, in some instances, law enforcement agencies have requested, and even paid for increased data retention. For example, three telecommunications carriers have been paid $1.8 million per year to provide the FBI with "near real-time access to [two years of stored] United States communications records (including telephone and Internet records)" [162]. Needless to say, although Verizon and AT&T received millions of dollars from the FBI to providing the FBI access to their customers' data, neither firm felt it necessary to inform their customers of the fact.

Similarly, between 2007 and 2008, MySpace and Facebook both increased their data retention periods for user login IP session data.[78] These social network sites did not publicly announce changes in their policies, nor did they update their privacy policies to reflect these rather significant shifts — likely because the privacy policies did not list the original data retention periods, let alone the new ones. Instead, the only disclosure of the changes were made in updated handbooks provided to law enforcement agencies.

[78] In 2006, MySpace logged IP addresses associated with account logins for 90 days. In 2007, the company expanded its logging of this data to 1 year [163, 164]. Likewise, Facebook logged IP addresses for 30 days in 2007, but by 2008, the company had lengthened its retention period to 90 days [165, 166].

6

Companies differ in their interpretation of privacy law

> "There's a whole [privacy] common law . . . that occurs today without the intercession of a legislator, an academic . . . a civil liberties person . . . or even the government. You know, every day decisions are made about what the law means by people who tend to be about 28 years old, may have graduated college, they typically say the same thing over and over again, and so repeat the insanity, if they did it wrong the first time, they'll do it wrong the next 52 times. Those are the people that work on the front line of most providers who receive the legal process and have to evaluate it and decide whether to give your email away or not" [10].
>
> —AL GIDARI

American privacy law, specifically, the Electronic Communications Privacy Act (ECPA), strictly regulates the circumstances in which providers can be forced to disclose their customers' data to third parties, such as law enforcement agencies. When a company receives a valid subpoena, a court order issued under 18 U.S.C. § 2703(d), or a search warrant, there is typically not much that the company can do to resist, should it wish to do so. Unless the order is invalid, the service provider must disclose the data to the requesting law enforcement agency. Even so, there are quite a few grey areas of the law that companies can exploit to protect the privacy of their customers, should they wish to do so. It is in these

grey areas where companies have the flexibility to interpret the law in the government's favor, or adopt pro-privacy policies that limit the reach of law enforcement agencies.

This chapter will delve into several obscure areas of the law and analyze the specific, often creative interpretations of privacy statutes adopted by some service providers. The fact that these companies have adopted strict readings of the law has, in many cases, never been publicly acknowledged by the firms, discussed by the press, or appeared in court records.

6.1 Opened e-mails and Theofel

18 U.S.C. § 2703(a) states that "a governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant." There has been considerable debate about the definition of the term "electronic storage," as the Department of Justice has taken the position that once an email message has been opened, such as by briefly reading it on a mobile device, it is no longer in electronic storage, and thus, a company can be forced to disclose it to the government with a mere subpoena or § 2703(d) order rather than with a warrant.[79]

The government's narrow interpretation of "electronic storage" was rejected by the Ninth Circuit Court of Appeals in *Theofel v. Farey-Jones*, in which the court held that email messages continue to be in "electronic storage" regardless of whether they have been previously accessed. Prosecutors within the Ninth Circuit are therefore bound by *Theofel*. However, the Department of Justice continues to argue that law enforcement agencies elsewhere may obtain opened emails with a subpoena even when the data sought is held on

[79] *See Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004).

servers located within the Ninth Circuit [167].

Many large Internet service providers take a different position. Some have argued that since their corporate headquarters are located within the Ninth Circuit, they must adhere to the *Theofel* precedent.[80] Others simply argue that they believe that *Theofel* is the correct interpretation of the law, and thus opened emails should not lose their legal protection, regardless of the location of the provider or the requesting government agency [168, 169]. In particular, both Microsoft and Yahoo have refused to comply with subpoenas or § 2703(d) orders for opened emails that are less than 181 days old, and have argued their respective positions in court. In some cases, they have been successful, and in others, they have not [170].

When providers receive a subpoena or § 2703(d) order from a law enforcement agency outside the Ninth circuit, they can either comply with the order or refuse and go to court. The companies that do refuse to comply rarely make this information public, and so it is exceeding difficult for consumers to easily evaluate a service provider's willingness to fight on this issue.

6.2 Delivering email headers in response to subpoenas

Internet service providers have quite a bit of flexibility to push back against government requests when the law is vague. One such example of this relates to the *to* and *from* headers in email messages that are over 181 days old and that are requested by law enforcement agencies using a subpoena.

18 U.S.C. § 2703(a) permits the government to use either a subpoena or a § 2703(d) order to compel the production of the contents of email communications that are older than 180 days. Non-content information, however, can only be obtained with a search warrant or a

[80] *See U.S. v. Weaver*, 636 F.Supp.2d 769 (C.D.Ill. 2009)

§ 2703(d) order.[81] E-mail headers have long been considered to be non-content (although this does not include the subject line), which the Ninth Circuit confirmed in *United States v. Forrester*.[82]

Over the last few years, Yahoo!, Google, and Microsoft have quietly adopted an aggressive legal theory, prioritizing the stronger legal protections that exist for non-content records than emails over 180 days old. As such, the companies now scrub the *to* and *from* headers from old email messages delivered to law enforcement agents in response to a subpoena.[83] In such scenarios, if law enforcement agencies wish to compel the disclosure of the headers from these three companies, they must first obtain a § 2703(d) order or search warrant. By adopting this creative, pro-privacy interpretation of the law, these service providers have been able to force some degree of judicial review over a process that would otherwise completely bypass the courts.

[81] 18 U.S.C. § 2703(c) specifies that "[a] governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (*not including the contents of communications*) only when the governmental entity — obtains a warrant ... [a 2703(d) order, or], has the consent of the subscriber or customer to such disclosure." A few specific categories of customer records can be obtained with a subpoena. Pursuant to 18 U.S.C. § 2703(c)(2)(a) — (f), these are, "name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number)."

[82] *See United States v. Forrester*, 512 F.3d 500, 503 (9th Cir. 2008).

[83] I have contacted representatives from most of the major email providers, but none would comment on-the-record about their interpretation of ECPA. Al Gidari, a private attorney who represents several service providers confirmed the fact that some service providers do in fact scrub the to and from headers, although he would not reveal which particular providers do so. However, based on interviews with several other knowledgeable sources, I believe that the practice originated at Yahoo!, under the direction of Richard Salgado, the company's legal compliance director. In 2010, Mr. Salgado left Yahoo! and went to work for Google. Shortly after he arrived at Google, the company adopted this reading of ECPA that Yahoo! had pioneered. Microsoft adopted a similar policy in May of 2010, after I alerted a senior member of the company's privacy team to the policy adopted by Yahoo! and Google.

6.3 Voluntary disclosures in emergency situations

While ECPA specifies the scenarios in which law enforcement agencies can compel service providers to disclose their customers' communications, it also allows for voluntary disclosure in emergencies.[84] 18 U.S.C. § 2702(b)(8) and 18 U.S.C. § 2702(c)(4) permit the disclosure of communications content and non-content: "to a governmental entity, if the provider, 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."[85]

Few companies will publicly discuss the extent to which they receive emergency requests and federal reporting requirements for such requests are largely worthless.[86] Even so, it is clear that the practice is widespread. For example, of the 88,000 lawful requests and demands Verizon received from federal, state and local officials in 2006, 25,000 were requests for emergency assistance [17].[87]

As the U.S. Internet Service Provider Association notes, "there is never an 'emergency' obligation on an ISP to disclose" [171]. If a service provider refuses to disclose, the government can always obtain a subpoena, a § 2703(d) order, or a search warrant, and compel the company to disclose the information. As such, a company's policy on emergency requests is one of the most useful indicators for its overall commitment to user privacy.

The area of voluntary disclosure is one of the most interesting, yet poorly understood

[84] The law has been repeatedly watered down over the past decade [46], often due to requests from telecommunications carriers who do not wish to be responsible for evaluating the degree of a particular emergency [85].

[85] There is little case law on the emergency provisions, although in general, once a service provider receives a statement from the government certifying the emergency, it can disclose the customers' communications without risk of liability. *See Jayne v. Sprint PCS*, No. CIV S-07-2522 (E.D. Cal. Feb. 20, 2009).

[86] There is a discussion of emergency disclosure reports in chapter 2.

[87] Of these 25,000 requests for emergency assistance, just 300 were from the federal government. Verizon has not released any statistics detailing how many of these 25,000 emergency requests it refused to comply with.

areas in which companies have complete and total control over the information they provide to law enforcement. The emergency disclosure policies of large providers vary quite a bit, although as a general matter, companies will not discuss them. Some companies, like AT&T, at least in some situations, appear to have taken the position that they will not disclose information to law enforcement agencies in emergencies.[88] In contrast, Verizon argued in court that it has a First Amendment right to voluntarily disclose its customers' private information to the National Security Agency [173].

Since companies are generally unwilling to describe their policies for voluntary disclosure of customer data, consumers have no real way to determine this information ahead of time when they evaluate a potential service provider or carrier.

6.4 Notifying users about law enforcement requests for their data

Federal law, specifically, 18 U.S.C. § 2703, outlines three general ways that law enforcement agencies can compel the disclosure of user data: search warrants, § 2703(d) orders, and subpoenas. With all three forms of legal process, the service provider may notify the user about the request, unless the government also seeks a court order under 18 U.S.C. § 2705(b) prohibiting the provider from doing so. However, while a provider *can* notify a user, it is not *required to* — the responsibility for notice, where it is required by law, lies with the government.

Notifying users (or threatening to do so) can protect their privacy in several ways. First, when law enforcement agencies request user data with a subpoena, a threat to notify

[88] In June 2009, an email message sent by a Florida police officer to others in the law enforcement community was published by WikiLeaks [172]. That email described the officer's experiences interacting with several Internet providers and telecom carriers during a recent child exploitation investigation. When presented with the same details describing the emergency situation, MySpace, Yahoo! and AT&T all had differing responses. MySpace immediately delivered the requested IP login information, Yahoo! pushed back, but eventually delivered IP logs, but only those for logins that were more than 48 hours old. In contrast, AT&T refused to voluntarily provide any customer information in response to the officer's request, and only delivered the requested records after the police obtained a subpoena that compelled disclosure.

the impacted user will force the law enforcement agency to go to court and seek an order to prohibit the notice. This threat draws a neutral judge into a process that would otherwise not have involved the courts, thus providing some degree of independent oversight. Second, providing a user with notice, when it occurs before their data has been shared with the law enforcement agency, gives the user the opportunity to fight the disclosure order [174, 175, 176, 177]. Third, there are several forms of compelled disclosure for which the government is not required to provide notice, including requests for stored communications content and non-content data.[89] As such, unless the service provider chooses to notify the user, they may never know that their data was sought and disclosed to law enforcement agencies.

Although companies are often free to notify their customers about law enforcement demands for their data, few companies do so, and those that do, do not always do it.[90] Even so, in recent years, several technology companies have adopted formal policies of notifying users whenever possible, unless prohibited from doing so by statute or court order.[91]

Notification policies, while admirable, do not automatically lead to transparency, as sealed surveillance orders are increasingly the norm [13, 14]. In such cases, companies can go the extra mile by seeking to unseal the orders. For example, between 2011 and 2012, Twitter, Google and Sonic.net were all presented with sealed § 2703(d) orders for

[89] The notice provisions in ECPA do not apply to requests for communications content pursuant to a search warrant. *See* 18 U.S.C. § 2703(b)(1)(A). Furthermore, at least one federal court has ruled that the notice requirements contained within Rule 41 of the Federal Rules of Criminal Procedure only require that the government provide notice to the service provider, not to the user whose communications were obtained. *See In re Application for Warrant*, Mag. No. 10-291-M-01 (D.D.C 2010). Likewise, the government does not have to provide notice to a surveillance target when it obtains their non-content data under 18 U.S.C § 2703(c), no matter the form of legal process used [178].

[90] One executive at a major service provider that chooses to notify users about requests on a case by case basis, told me that "we don't want to notify a pedophile who is trying to lure a teen through our site, but we do want to notify [Martin Luther King, Jr.] if the FBI is asking for records."

[91] These include Twitter, Dropbox, LinkedIn, Sonic.net and SpiderOak [158, 159, 160, 107, 179]. Google has pledged to notify its users whenever possible, but this commitment was made only in a blog post and a difficult-to-find FAQ, rather than in a formal written policy [180].

records about their customers as part of the FBI's investigation into WikiLeaks. The order to Twitter was unsealed at the company's request [174]; Google and Sonic.net also sought to have the orders unsealed, but were unsuccessful [176].

6.5 Stretching the definition of communications "content"

> "Content is content, I don't care how many times you try to repackage it into something else, content is still content, and the standards that we try to apply that give lesser protection to that content inevitably falls short, as well, when people stop and think about it" [10].
>
> —AL GIDARI

> "[If] you look at new services like search that both Google and Microsoft provide, and the question is how [ECPA] applies under these definitions. I mean, looking at the definitions you would have no idea. There are arguments that could be made in different ways. [W]e think probably the best interpretation of search under ECPA is that the query itself would be content" [181].
>
> —MIKE HINTZE, ASSOCIATE GENERAL COUNSEL, MICROSOFT

Under the Electronic Communications Privacy Act, the legal process required to compel the disclosure of user data varies depending on the type of data. Specifically, if law enforcement agents are seeking "the contents of any wire or electronic communication," then a probable cause warrant is generally required.[92] If, on the other hand, the government wishes to obtain "a record or other information pertaining to a subscriber," a § 2703(d) order is sufficient, which is much easier to get. Although the statute recognizes these two different categories of information, it does not define them.[93]

[92] As long as the data is still in "electronic storage." *See* 18 U.S.C. § 2703(b)(1).

[93] In addition to the warrant protections for content under ECPA, the United States Court of Appeals for the Sixth Circuit ruled in 2010 that individuals have a reasonable expectation of privacy in the contents of their email messages which are therefore protected by the Fourth Amendment. *See United States v. Warshak*, 631 F.3d 266, (6th Cir. 2010).

Some services, like e-mail and instant messaging already existed at the time that ECPA was drafted, and so although the term e-mail does not appear in the statute, it is relatively easy for lawyers to agree that such communications are content under ECPA. Other technologies were not invented until far more recently, and so it is not entirely clear whether they are communications content or non-content.[94] Examples of this include search engine queries, location information (when shared with friends via "check-in" services like Foursquare), as well as interactions on social networks like Facebook.

As with the other examples in this chapter, where the law is vague, some companies have adopted aggressive interpretations of the law in order to limit the ease with which law enforcement agencies can obtain their customers' data. When communications content is the only category of data that receives the highest degree of privacy protection under the law, providers wishing to shield their users' data from warrantless government access will attempt to argue, whenever possible, that the data in their possession is communications content. As such, Google and Microsoft have both taken the position that search queries are content.[95] Likewise, Google and Loopt have taken a similar position with regard to user supplied location data [184]. Facebook has also taken a fairly aggressive stance, arguing that much of the data that users upload to the service is content, such as messages,

[94] As Richard Salgado, Google's Director of Law Enforcement and Information Security, observed during testimony before a congressional committee in 2010, "ECPA was written for the communications and computer technology of 1986. The ways in which we communicate and compute today, however, bear little resemblance to those of a quarter century ago . . . Moreover, providers, judges and law enforcement alike have difficulty understanding and applying the law to today's technology and business practices" [182].

[95] As I understand it, prior to the *Warshak* decision, both Google and Microsoft took the position that search queries were communications content under ECPA. Since then, several technology companies appear to have pivoted. They still require a warrant, but do so by relying on Warshak and the Fourth Amendment, rather than ECPA. For example, Google's Richard Salgado revealed in 2012 that "most providers now, although I really should only speak to Google, view the way the case law is going and certainly viewing the Fourth Amendment as applying to any content that is provided by the user to the service. So that, for Google, would include things like Calendar and Docs, and all those others, even where there is not a communication function going on. That there's not another party involved in the Doc that you're uploading, the notes that you're keeping for yourself. It's still material that you've put with the service provider as part of the service that the company, in this case Google, is holding on your behalf. It's our view that that is protected by the Fourth Amendment, and unless one of the exceptions to the warrant requirement apply, it's not to be disclosed to a government entity as a matter of compulsion" [183].

photos, videos, and wall posts [106].

Unsurprisingly, the law enforcement community often does not share the same view of the law as these companies. For example, the general counsel of the FBI has stated that she believes location information of the kind shared by users with Google, Foursquare and Loopt is non-content, and does not require a warrant to obtain [10]. However, it remains unclear if these companies have received requests for location data, or whether their legal theories have been tested in court.

7

A failed market for privacy?

Across corporate America, companies have seemingly come to recognize the importance of privacy. Practically every corporate website has a privacy policy and the majority of Fortune 500 companies have appointed a Chief Privacy Officer [185]. In statements to consumers and the press, most companies pledge to value and respect their customers' privacy. Some companies even claim to compete on privacy [186], most visibly, the major search engines and web browser vendors, deploying, respectively, ever-more privacy-protecting data retention policies and anti-tracking technologies [187, 188].

Although companies routinely proclaim that they care about privacy, they are rarely willing to discuss the details surrounding law enforcement and intelligence agencies' access to their customers' data, or the degree to which they proactively assist, or resist such access. This is unsurprising, as few companies effectively protect their customers' data from the government. Any in-depth, honest discussion of the topic would therefore risk alarming consumers [50, 110], and perhaps give them a reason to share less private data with service providers.

Furthermore, in many cases, telecommunications carriers and Internet service providers that have publicly pledged to protect user privacy have instead voluntarily assisted and facilitated government access to their customers' most private information.

For example, even though Verizon claims it has a "longstanding and vigorous commitment to protecting its customers' privacy" [17], the company argued in court that it has a First Amendment right to voluntarily provide information about its customers' private communications to the National Security Agency [173]. Even if this is a valid legal position, it is in no way consistent with the company's statements about protecting its customers' privacy. Furthermore, to the extent that Verizon has embraced a corporate philosophy of putting the government's surveillance needs first, the company has certainly not advertised this to the public via its website, nor is this information provided to members of the public that visit the wireless carrier's retail stores.

Likewise, Google has made bold statements about the "trust our users place in us, and our responsibility to protect that privacy" [189]. The company also has a YouTube privacy channel with over fifty videos describing the privacy features built into its products, including one that promises that the company "makes privacy a priority in everything we do" [190]. Yet, in spite of these admirable efforts to educate consumers about the company's privacy practices, none of Google's privacy videos disclose that one of the main reasons the company retains identifying user log data is so that it may deliver it to the government [149].

Finally, Microsoft has pledged that it takes its "customers' privacy seriously" [191]. However, when asked if the company was considering a policy to log no search data at all, Peter Cullen, Microsoft's chief privacy strategist, told a journalist in 2007 that too much privacy is dangerous. "Anonymized search," he said, "can become a haven for child predators. We want to make sure users have control and choices, but at the same time, we want to provide a security balance" [150]. However, Microsoft does not disclose on its website or in its privacy policy that the company balanced the needs of law enforcement agencies against its customers' privacy in choosing its data retention period (let alone that the needs of the government took priority).

This is not an attempt to pick on a few companies — the examples I have highlighted are in fact quite typical for the telecommunications industry. With few exceptions, the large companies to whom hundreds of millions of consumers entrust their private communications actively assist in the collection and disclosure of that data to law enforcement and intelligence agencies — all while simultaneously promising to protect their customers' privacy.

These firms are not necessarily hostile to privacy. Rather, when they speak about their commitment to protecting their customers' privacy, what they really mean is that they will not improperly use or access that data for commercial purposes. That these companies have adopted an extremely limited definition of privacy is not made clear to consumers, who might reasonably believe that when these firms say that they protect their customers' privacy, it is from all threats, and not just a select few from private actors.

While most companies will not discuss their interactions with the government, it would be unfair to say that companies are all equal in the degree to which they assist government agencies and the extent to which their products and policies shield user data from the government — rather, they rarely discuss these differences, and never compete on them. Consequently, this chapter will seek to explore the lack of competition among major service providers for privacy protections that effectively thwart government access to user data.

7.1 Protecting privacy can conflict with free business models

> "We couldn't run our system if everything in it were encrypted [in storage] because then we wouldn't know which ads to show you. So this is a system that was designed around a particular business model" [147].
>
> —VINT CERF, VICE PRESIDENT AND CHIEF INTERNET EVANGELIST, GOOGLE

As I have documented in chapters 5 and 6 of this dissertation, there are many ways for companies to shield their customers' data from the government. Some of these involve the adoption of privacy by design, such as through the use of encryption technologies or minimal data retention policies, while others involve the adoption of novel and often aggressive legal theories that force law enforcement agencies to obtain and demonstrate greater evidence of a crime before they can compel the company to disclose data.

While none of these privacy protections are free, some come at a higher cost to the companies that employ them. Specifically, while some methods require the assistance of outside legal experts, additional engineering resources or specialized hardware, such as cryptographic accelerators used to speed up transport encryption, they do not prevent service providers from making money. In contrast, privacy protections such as minimal data retention or encryption of stored data directly conflict with the dominant Silicon Valley business model in which large amounts of user data are collected, analyzed and monetized. Consequently, firms like Google and Facebook that offer free services to consumers in order to collect their data are far more likely to embrace privacy protection methods that are complimentary to their business models, such as by adopting aggressive, pro-user legal positions in their interactions with the government. In contrast, these firms are unlikely to willingly embrace minimal data retention policies or encrypt stored user data in such a way that they can no longer access it.

Consider the example of storage encryption: It is exceedingly difficult for companies to monetize datasets that they cannot analyze. Google's popular Gmail service scans the text of individual emails, and algorithmically displays relevant advertisements next to the email. When a consumer receives an email from a friend relating to vacation plans, Google can display an advertisement for hotels near to the destination, rental cars or travel insurance. If those emails are encrypted with a key not known to Google, the company cannot

scan the contents and display related advertising.[96]

Google, Microsoft and Facebook offer free services to hundreds of millions of users. These companies are not charities, staffed by volunteer labor; they employ thousands of highly paid engineers and own or lease data centers filled with millions of servers. Rather than charge their users a fee, the firms have opted to monetize their users' private data. As a result, any move to shield this data will directly impact the companies' ability to monetize it and thus return a profit to their shareholders [193]. Barring some revolutionary developments from the cryptographic research community,[97] advertising based business models are fundamentally incompatible with online data storage services that encrypt data with keys only known to their users. Of course, mining user data in order to deliver behavioral advertising is not the only way to pay for products — however, it is the dominant model adopted by most online services.

7.2 When and why are companies likely to say no to the government?

If companies decide to retain private user data, at some point, they will receive a request for it from the government [197]. Once a service provider does receive a request for user data in its possession, the time for technology based protection methods has past — the only thing standing between the data and the government is the company's legal team, and their willingness to fight.

Yet, in spite of the fact that major technology and communications companies all have

[96] The company can, of course, display generic advertisements unrelated to the user's communications contents, but these will be far less profitable [192].

[97] Researchers have in recent years proposed several privacy-preserving behavioral advertising systems, none of which have been adopted and deployed by advertising companies [194, 195, 196]. Furthermore, these schemes are largely focused on advertising based on consumers' Internet browsing habits, rather than private communications data stored with cloud computing providers.

large legal teams, they differ in their willingness to resist the government. Some push back against requests that are overbroad, some seek to notify the user before disclosing their data [174, 176], while others go out of their way to assist the government, in some cases, knowingly facilitating wholesale, illegal surveillance of their customers [198, 93].

The phrase "if you aren't paying for the product, you are the product" has in recent years become a popular meme among privacy advocates, the media, and even politicians [199, 200]. There may be some truth in it, at least with regard to the ways in which companies like Google and Facebook will do practically anything to collect consumers' private data. Even so, one might normally expect companies to aggressively protect the privacy of their paying customers while offering little resistance when the government requests the data of those users who free ride. Yet, the actual practices of major service providers suggests the contrary — that when it comes to the degree to which companies resist government requests for their customers' data, paying a provider doesn't automatically lead to greater privacy.

Consider, for example, that several of the largest telephone carriers in the United States knowingly and voluntarily assisted the National Security Agency in illegally spying on the communications of millions of their paying customers [198]. In contrast, as I documented in chapter 6, Google, Facebook and Twitter's legal teams have aggressively resisted requests from the government for their customers' data — even though the vast majority of their customers have not paid a dime for the services provided to them.

How can we explain the reluctance of the telephone companies to protect their paying customers and the willingness of technology firms to fight to protect customers who've never written them a check? I believe there are several likely reasons.

First, companies that monetize user data such as Facebook and Google have much to lose if consumers lose faith in the firms' ability to protect their private information from the government. These companies have an enormous appetite for highly sensitive data,

such as communications content, geo-location records, and social graphs. Their business models depend upon continued access to a firehose of private user information, which they monetize through targeted advertising. Over the past several years, many technology companies have made privacy related missteps by over-collecting or under-protecting the data entrusted to them [201, 202, 203], drawing the attention of legislators [204, 205, 206], regulators [207, 208, 209] and class action lawyers [210, 211, 212]. For Facebook and Google in particular, once occasional privacy scandals have become a regular occurrence. While these companies are not intentionally drawing media attention to their privacy invading business practices, the scandals are at least associated with profitable data collection practices. A privacy scandal every month, although certainly unpleasant, may merely be the cost of doing business.

In contrast, service providers do not generally profit by helping the government; if anything, they lose money providing surveillance assistance. These companies do not want consumers to be so scared of government access that they take steps to prevent the firms from collecting and retaining their private data [50]. Therefore, by publicly resisting the government's surveillance efforts, these companies can avoid giving consumers yet another reason to stop trusting them.

Second, firms in heavily regulated industries, such as the telecommunications industry, cannot afford to aggressively and publicly do battle with law enforcement agencies. As Silicon Valley firms grow from small start-ups to billion dollar technology giants, they become vulnerable to the whims of members of Congress, the FBI, NSA and other executive agencies. Law enforcement agencies can exert considerable pressure on service providers. In some cases, they can slow down or block the introduction of new products,[98]

[98] According to Stewart Baker, the former General Counsel of the National Security Agency, "[t]he FBI and the Justice Department have intervened repeatedly at the [Federal Communications Commission] to try to deny licenses to companies that have not been fully cooperative or that have developed new technologies that the FBI thinks should be more accessible [to surveillance]. This is all in an effort to get the FCC, usually successfully, to deny licenses to operate in the United States to companies that have not cooperated with the Bureau. They did this to Iridium when Iridium wanted to locate a ground station in Canada. They did it in the

seize providers' servers during investigations rather than requesting that the company simply make a copy of and deliver user data [214], or use their lobbying power to push for Congress to pass legislation that will limit a company's ability to make money.[99]

Legislators also have a significant amount of power over companies. Telecommunications carriers are highly regulated entities with matters such as spectrum acquisition and mergers that are regularly before congressional committees. Technology companies like Google, Facebook and Microsoft also depend upon the goodwill of Congress — whether they are attempting to fight Hollywood's attempts to expand copyright law, telecommunications networks wishing to eviscerate net neutrality rules, or because of the increasingly frequent privacy scandals related to their own use of consumer data.

Accepting the realities of Washington DC, large companies eventually bow to the needs of law enforcement, the intelligence community, and their friends in Congress. Thus, even though Facebook and Google have adopted aggressive, pro-privacy legal theories in order to resist law enforcement requests for user data, neither firm has publicly lobbied against data retention legislation or expanded lawful access requirements [35, 217]. High-profile feuds with law enforcement interests will consume valuable political capital that the firms must preserve for other, more important issues.

BT-MCI merger. And it has become a regular feature of mergers where foreign companies propose to provide telecommunications services in the United States" [213].

[99]The Electronic Communications Privacy Act does not prohibit service providers from sharing or selling their customers' communications metadata with other companies. At a Senate ECPA reform hearing in 2011, Associate Deputy Attorney General James Baker suggested that Congress should consider prohibiting such commercial disclosures. He also suggested that the provisions in ECPA requiring compensation to providers for the time and manpower it takes to comply with surveillance requests should also be revisited [215]. Julian Sanchez has speculated that these two proposals, both of which would hurt service providers, were designed to punish companies for joining with consumer advocates and civil liberties groups in calling for reform of ECPA [216].

7.3 Privacy as a shrouded attribute

> "Some in the privacy community have said, if only we knew those [differing law enforcement and privacy] policies, people could make rational decisions on which provider to use. Would you use — I won't pick names, but you can pick out one or two big carriers, would you use them if you knew they were rolling over and giving everything to the government without looking twice, or would you go to somebody that used encryption or security or data and applied the strictest rules possible? Well . . . that's a good question" [10].
>
> —AL GIDARI

> "If consumers cannot easily obtain information about a product's safety (but can easily observe its price), price competition may reward those who cut their price by offering a less safe product" [218].
>
> —HOWARD BEALES ET AL, FEDERAL TRADE COMMISSION

The privacy protecting policies and technologies adopted by companies are typically *shrouded*. Data retention policies are rarely disclosed, the use of transport encryption is observable, but typically overlooked by most consumers [219], while the methods used to encrypt data in storage cannot be directly verified by consumers. Likewise, firms rarely discuss the obscure, yet important legal positions they have adopted or the degree to which they request financial compensation from law enforcement agencies before disclosing user data.[100] As such, details about most of the important privacy practices adopted by firms are not public, nor available to consumers when they are evaluating the products offered by competing service providers.

In their seminal work analyzing markets with shrouded attributes, such as printer ink refills and free checking accounts, economists Xavier Gabaix and David Laibson noted

[100] It has taken me several years to discover the legal positions described chapter 6. Much of the information I have obtained has been through trusted relationships I have established with lawyers working for service providers and the government, often over drinks in Washington D.C. bars. This method of information discovery is, for obvious reasons, simply not an option for the average consumer.

that consumers rarely consider the full cost of these products as they do not calculate in the added costs of shrouded attributes.[101] This can lead to two forms of exploitation in the market: First, optimizing firms exploit myopic consumers through marketing schemes that shroud high-priced add-ons. Second, sophisticated consumers then exploit these marketing schemes. Thus, by hiding the true cost of a product, a firm can offer the good at a lower initial price, since it will be able to recoup any lost profit via shrouded after sale fees. Savvy consumers can take then advantage of this if substitute add-on goods (such as generic printer ink refills) are available.

The paradox that Gabaix and Laibson identified is that manufacturers have no incentive to abandon the shrouded goods model, offer fairly priced goods, and highlight the nefarious business practices employed by their competitors. This is because each consumer educated about the shrouded attributes, rather than flocking to vendors pricing their goods fairly, will instead purchase cheap after-market substitutes, and continue to purchase the subsidized shrouded good.

Shrouded attributes are not limited to the market for printer ink. In fact, many privacy and security aspects to online applications and communications services are shrouded. When consumers evaluate these products, they likely consider the cost, usability, speed and perhaps weigh in social factors — such as the number of their friends who are currently using them. Consumers are unlikely to consider the encryption methods used by the services,[102] the data retention policies adopted by the firms, or the extent to which the companies resist government demands.

Companies like Google, Facebook, AT&T or Verizon have little to gain by highlighting their own privacy problems. Without regulatory pressure (something unlikely in the

[101] Gabaix and Laibson observe that "consumers sometimes fail to anticipate contingencies. When consumers pick among a set of goods, some consumers do not take full account of *shrouded product attributes*, including maintenance costs, prices for necessary add-ons, or hidden fees ... Shrouded attributes may include surcharges, fees, penalties, accessories, options, or any other hidden feature of the ongoing relationship between a consumer and a firm" [220].

[102] Particularly since most are not even aware of the existence of encryption when it is offered [219].

United States, where no regulator has the responsibility to protect the public from government surveillance) these firms will unfortunately, continue to shroud the privacy impacting aspects of their products and policies. Without reform, there will be no effective market for privacy protections from the government.

8

Future work

This dissertation scratches the surface of third-party assisted surveillance performed by U.S. government agencies. While I have spent more than six years collecting the data presented here, there remain far more unanswered questions than those for which I know the answer. Scholars, activists, journalists and hopefully, Congress, will in the future expose to sunlight the many other ways our government increasingly monitors every aspect of our lives. For example, we know practically nothing about our government's surveillance of banking and credit card transactions, public transportation and toll booth transaction records, or the extent to which it obtains records from public utility companies.[103] In addition to not knowing about the scale of requests such, we often do not know the legal theories adopted by the government [222]. Finally, although several Senators have made it clear that *something is rotten in the state of Denmark* [223, 224], the public knows practically nothing about how intelligence agencies use their surveillance powers, or even how they interpret the law.

Surveillance is a growth industry about which we know very little. The silver lining to this is that there is no shortage of interesting topics for researchers to study. The challenge will be to build relationships with sources and convince them to talk.

[103] In 2011, the California Public Utilities Commission adopted privacy rules which will require utility companies to compile and submit reports detailing the number of times they were forced to disclose their customers' information to third parties, including law enforcement agencies [221]. These reports will reveal, for the first time, data regarding the scale of this form of law enforcement surveillance.

9

Conclusion

In this dissertation, I have documented the central role that third party communications service providers now play in the surveillance of their customers by law enforcement agencies. Quite simply, these firms power the surveillance state in which we now live. Without their assistance, the government would be wholly unable to get the depth of data it desires, at the scale it now demands. For large companies, surveillance is now an inescapable responsibility. Often, their assistance is required by law, and when it isn't, the government can usually apply sufficient pressure to get the companies to bend.

Over the past few decades, the scale of electronic communications surveillance has quietly grown from a few thousand requests to more than one and a half million requests each year. During this time, the government has gained access to new sources of data and economies of scale made possible through the shift to automated surveillance. Meanwhile, the public, Congress and the courts remain largely in the dark. Those who have watched the expansion of the surveillance state and who understand its scale — the surveillance teams within the companies, their lawyers, and law enforcement officials — rarely talk. For the companies that collect consumers' data and the government agencies that seek to obtain it, there is little to be gained by discussing such topics. The companies fear scaring away consumers, while those in the government wish to avoid educating criminals and the general public about the reach and limitations of their surveillance capabilities.

Year after year, the number of surveillance requests received by the companies grows at double-digit rates, while at the same time, the incentives of the companies and government are aligned to shield this information from the public. With every new free communications service, social app, or mobile technology, more private data about individuals ends up in the hands of companies. Eventually, law enforcement agencies will demand this data and the companies will be obligated to hand it over, often without ever telling the impacted users.

Companies can take steps to limit the extent to which they actively facilitate government surveillance, should they wish to do so. Minimal data retention policies can be adopted, strong encryption built into products, and legal teams directed to fight on behalf of users. Unfortunately, few companies have taken such steps, particularly those in heavily regulated markets or those that collect and monetize user data. Fighting the government — or even prioritizing the privacy of users over the surveillance apparatus — is bad for business.

The symbiotic surveillance alliance between the large companies and the government has been able to exist and frankly, to fester, because of secrecy. Because the public does not know how much of their data is collected and retained by these companies, and because they do not understand how much of it or how frequently it is delivered to the government. Under such conditions, starved of sunlight, it is no surprise that the interests of users are not represented.

If there is any hope that politicians and the courts will take on law enforcement interests, it will be as a result of increased transparency. Once those in power learn how much of their own communications, location data, and other private information has ended up in government databases, they may be more likely to act. This dissertation is just one step along the path to exposing and restraining the surveillance apparatus.

Bibliography

[1] Franklin D. Roosevelt. Memorandum for the Attorney General. May 21 1940. Included as Appendix I in *United States v. White*, 401 U.S. 745, 766 (1971) (Douglas, J., Dissenting).

[2] Jan Whittington and Chris Jay Hoofnagle. Unpacking Privacy's Price. *North Carolina Law Review*, 90:1327, 2012.

[3] Whitfield Diffie and Susan Landau. Communications surveillance. *Communications of the ACM*, 52(11):42, November 2009.

[4] Paul Ohm. The Fourth Amendment in a World Without Privacy. *Mississippi Law Journal*, 81:1309, 2012.

[5] Saul Hansell. Increasingly, Internet's Data Trail Leads to Court. *The New York Times*, February 4 2006. `www.nytimes.com/2006/02/04/technology/04privacy.html`.

[6] Albert Gidari. Companies Caught in the Middle. *University of San Francisco Law Review*, 41(4):535, 2007.

[7] Todd M. Hinnen. Statement of Acting Assistant Attorney General for National Security at the Department of Justice. *Hearing on "Permanent Provisions Of The PATRIOT Act," House Judiciary Committee, Subcommittee on Crime, Terrorism, And Homeland Security*, page 69, March 30 2011. `judiciary.house.gov/hearings/printers/112th/112-15_65486.PDF`.

[8] Michael Altschul. Balancing Government's Needs with Customer Needs. *Law Review of Michigan State University Detroit College of Law*, 2002:787, 2002.

[9] Declan McCullagh. How safe is instant messaging? A security and privacy survey. *CNET News*, June 9 2008. news.cnet.com/8301-13578_3-9962106-38.html.

[10] James A. Baker, Valerie E. Caproni, James Dempsey, and Albert Gidari. Reforming the Electronic Communications Privacy Act (Panel). *The Brookings Institution*, May 17 2011. www.brookings.edu/~/media/Files/events/2011/0517_electronic_privacy/20110517_electronic_privacy.pdf.

[11] Kashmir Hill. Facebook's Top Cop: Joe Sullivan. *Forbes*, February 22 2012. www.forbes.com/sites/kashmirhill/2012/02/22/facebooks-top-cop-joe-sullivan.

[12] Christopher Soghoian. 8 Million Reasons for Real Surveillance Oversight. *Slight Paranoia (Blog)*, December 1 2009. paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html.

[13] Stephen W. Smith. Kudzu in the Courthouse: Judgments Made in the Shade. *Federal Courts Law Review*, 3:177, 2009.

[14] Stephen W. Smith. Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket. *Harvard Law & Policy Review*, 6, 2012.

[15] Ronald Weich. Letter from Assistant Attorney General, Office of Legislative Affairs, Department of Justice to Joseph R. Biden, Jr. April 30 2012. www.fas.org/irp/agency/doj/fisa/2011rept.pdf.

[16] Patrick Leahy. Statement of U.S. Senator During Debate Over "The Continued Reporting of Intercepted Wire, Oral, and Electronic Communications Act". page 30868, November 19 1999. www.gpo.gov/fdsys/pkg/CRECB-1999-pt21/pdf/CRECB-1999-pt21.pdf.

[17] Randal S. Milch. Letter from General Counsel, Verizon Business to John D. Dingel, Edward J. Markey and Bart Stupak, U.S. Reps. October 12 2007. web.archive.org/web/20080228053451/http://markey.house.gov/docs/telecomm/Verizon_wiretaping_response_101207.pdf.

[18] Department of Justice. Report on the use of pen registers and trap and trace devices by the law enforcement agencies/offices of the Department of Justice for calendar year 2009. files.spyingstats.com/pr-tt/doj-high-level-pr-tt-2009.pdf.

[19] Administrative Office of the U.S. Courts. Wiretap Reports. www.uscourts.gov/Statistics/WiretapReports.aspx.

[20] U.S. Senate. Senate Report: Omnibus Crime Control and Safe Streets Act of 1968. June 19 1968.

[21] Electronic Privacy Information Center. Title III Electronic Surveillance 1968-2010. July 6 2011. epic.org/privacy/wiretap/stats/wiretap_stats.html.

[22] Julian Sanchez. Our Wiretap Data Is Getting Worse. *CATO @ Liberty*, July 11 2012. www.cato-at-liberty.org/our-wiretap-data-is-getting-worse.

[23] Paul Ohm. Email to Christopher Soghoian. April 8 2011. On file with author.

[24] James M. Cole. Letter from Deputy Attorney General, Department of Justice to Chairman Darrell Issa et al., House Committee on Oversight and Government Reform. *Published in Committee Report 112–546*, page 10, January 27 2012. www.gpo.gov/fdsys/pkg/CRPT-112hrpt546/pdf/CRPT-112hrpt546.pdf.

[25] Pew Internet and American Life Project. A closer look at generations and cell phone ownership, February 3 2011. www.pewinternet.org/Infographics/2011/Generations-and-cell-phones.aspx.

[26] Jeffrey Reiman. *The Rich Get Richer and the Poor Get Prison*, page 81. MacMillan Publishing Company, 1990.

[27] Ryan Singel. DCS-3000 is the FBIs new Carnivore. *Wired*, April 27 2006. `www.wired.com/threatlevel/2006/04/dcs3000_is_the_`.

[28] Jim Dwyer. It's Not Just Drug Dealers Who Buy Prepaid Phones. *The New York Times*, May 30 2010. `www.nytimes.com/2010/05/30/nyregion/30about.html`.

[29] George W. Bush. Speech by President, United States of America, Buffalo, NY, April 20 2004. `rawstory.com/news/2005/Bush_claimed_taps_required_warrants_in_1220.html`.

[30] Lisa A. Judge. FOIA Response to ACLU from Principal Assistant City Attorney, Tucson Police Department (Containing Surveillance Price Lists for Various Wireless Carriers). September 6 2011. `www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_tucsonpd_tucsonaz.pdf`.

[31] Google. Invoice to US Marshals Service Re: Pen Register/Trap Trace, January 4 2008. `files.cloudprivacy.net/Yahoo-invoices-2.pdf`.

[32] Kim Zetter. Yahoo Issues Takedown Notice for Spying Price List. *Wired*, December 4 2009. `www.wired.com/threatlevel/2009/12/yahoo-spy-prices`.

[33] Louis J. Freeh. Statement of Director, Federal Bureau of Investigation Before the Senate Judiciary Committee, July 9 1997. `epic.org/crypto/legislation/freeh_797.html`.

[34] Declan McCullagh. Congress Mulls Stiff Crypto Laws. *Wired*, September 13 2001. `www.wired.com/politics/law/news/2001/09/46816`.

[35] Charlie Savage. U.S. Tries to Make It Easier to Wiretap the Internet. *The New York Times*, September 27 2010. `www.nytimes.com/2010/09/27/us/27wiretap.html`.

[36] Ryan Singel. FBI Drive for Encryption Backdoors Is Déjà Vu for Security Experts. *Wired*, September 27 2010. www.wired.com/threatlevel/2010/09/fbi-backdoors.

[37] U.S. Senate. Senate Report: Electronic Communications Privacy Act of 1986. October 17 1986. www.justice.gov/jmd/ls/legislative_histories/pl99-508/senaterept-99-541-1986.pdf.

[38] Paul M. Schwartz. Reviving Telecommunications Surveillance Law. *University of Chicago Law Review*, 75:287, 2008.

[39] David Kravets. Congress Left in Dark on DOJ Wiretaps. *Wired*, February 13 2012. www.wired.com/threatlevel/2012/02/congress-in-the-dark.

[40] Nancy Libin. Email from Chief Privacy and Civil Liberties Officer, Office of the Deputy Attorney General, Department of Justice to Christopher Soghoian. September 3 2010. On file with author.

[41] Electronic Privacy Information Center. Approvals for Federal Pen Registers and Trap and Trace Devices 1987–1998. www.epic.org/privacy/wiretap/stats/penreg.html.

[42] Rena Y. Kim. Letter from Chief, FOIA Unit, Office of Enforcement Operations, Criminal Division, Department of Justice to Kevin Bankston, June 5 2008. files.spyingstats.com/pr-tt/doj-details-pr-tt-1999.pdf.

[43] Nancy Libin. Email from Chief Privacy and Civil Liberties Officer, Office of the Deputy Attorney General, Department of Justice to Christopher Soghoian. October 13 2010. On file with author.

[44] Aaron Koepper. ACLU Sues DOJ For Digital Surveillance Data. *Main Justice*,

May 24 2012. www.mainjustice.com/2012/05/24/aclu-sues-doj-for-electronic-surveillance-data.

[45] Marc Rotenberg. Letter to Senator Leahy Re: FBI Reporting Concerning Pen Register/Trap and Trace Statistics. April 29 2009. epic.org/privacy/wiretap/ltr_pen_trap_leahy_final.pdf.

[46] Seth Rosenbloom. Crying Wolf in the Digital Age: Voluntary Disclosure Under the Stored Communication Act. *Columbia Human Rights Law Review*, 39:529, 2007.

[47] House Judiciary Committee. Committee Report: USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005. page 121, July 18 2005. www.gpo.gov/fdsys/pkg/CRPT-109hrpt174/pdf/CRPT-109hrpt174-pt1.pdf.

[48] Richard S. Hertling. Letter from Acting Assistant Attorney General, Office of Legislative Affairs, Department of Justice to Senator Patrick Leahy. April 9 2007. files.spyingstats.com/exigent-requests/doj-2702-report-2007.pdf.

[49] Ryan Singel. Google, Microsoft Push Feds to Fix Privacy Laws. *Wired*, March 30 2010. www.wired.com/threatlevel/2010/03/google-microsoft-ecpa.

[50] Michael T. Gershberg. Letter from Counsel to Yahoo! Inc to William Bordley, U.S. Marshals Service. September 15 2009. files.cloudprivacy.net/yahoo-price-list-letter.PDF.

[51] Ben Worthen. Data Privacy: What to Do When Uncle Sam Wants Your Data. *CIO*, April 15 2003. www.cio.com/article/print/31836.

[52] Nick Summers. Walking the Cyberbeat. *Newsweek*, April 30 2009. www.thedailybeast.com/newsweek/2009/04/30/walking-the-cyberbeat.html.

[53] Nate Anderson. Time Warner Cable tries to put brakes on massive piracy case. *Ars Technica*, May 15 2010. arstechnica.com/tech-policy/2010/05/time-warner-cable-tries-to-put-brakes-on-massive-piracy-case/.

[54] Google. Transparency Report, Frequently Asked Questions, 2012. www.google.com/transparencyreport/faq/.

[55] Dropbox. Transparency Report. 2012. www.dropbox.com/transparency.

[56] Ethan Oberman. Increasing Transparency Alongside Privacy. *From the Treetops*, May 7 2012. spideroak.com/blog/20120507010958-increasing-transparency-alongside-privacy.

[57] Dane Jasper. Transparency Report. *Sonic.net CEO Blog*, April 13 2012. corp.sonic.net/ceo/2012/04/13/transparency-report.

[58] LinkedIn. Government Data Request Statistics. May 22 2012. help.linkedin.com/app/answers/detail/a_id/21733.

[59] Jeremy Kessel. Twitter Transparency Report. *twitter blog*, July 2 2012. blog.twitter.com/2012/07/twitter-transparency-report.html.

[60] Ellen Nakashima. Cellphone Tracking Powers on Request. *The Washington Post*, November 22 2007. www.washingtonpost.com/wp-dyn/content/article/2007/11/22/AR2007112201444.html.

[61] Declan McCullagh. Feds push for tracking cell phones. *CNET News*, February 11 2010. news.cnet.com/8301-13578_3-10451518-38.html.

[62] Stephanie K. Pell and Christopher Soghoian. Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact. *Berkeley Technology Law Journal*, 27:117, 2012.

[63] Michael Isikoff. The Snitch in Your Pocket. *Newsweek*, February 18 2010. www.thedailybeast.com/newsweek/2010/02/18/the-snitch-in-your-pocket.html.

[64] Christopher Soghoian. ACLU docs reveal real-time cell phone location spying is easy and cheap. *Slight Paranoia (Blog)*, April 3 2012. paranoia.dubfire.net/2012/04/aclu-docs-reveal-real-time-cell-phone.html.

[65] Eric Lichtblau. More Demands on Cell Carriers in Surveillance. *The New York Times*, July 8 2012. www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html.

[66] Paul Kirby. Wireless Carriers Report Increase In Law Enforcement Record Requests. *TR Daily*, July 9 2012. arstechnica.com/tech-policy/2010/05/time-warner-cable-tries-to-put-brakes-on-massive-piracy-case/.

[67] Erin Bush. FAQs About Neustar and Our Assistance to Law Enforcement. *Neustar Insights (Blog)*, July 17 2012. blog.neustar.biz/neustar-insights/faqs-about-neustar-and-our-assistance-to-law-enforcement/.

[68] Vonya B. McCann. Letter from Senior Vice President, Government Affairs, Sprint Nextel to Edward J. Markey, U.S. Rep. May 23 2012. markey.house.gov/sites/markey.house.gov/files/documents/Sprint%20Response%20to%20Rep.%20Markey.pdf.

[69] Timothy P. McKone. Letter from Executive Vice President, Federal Relations, AT&T Services, Inc. to Edward J. Markey, U.S. Rep. May 29 2012. markey.house.gov/sites/markey.house.gov/files/documents/AT%26T%20Response%20to%20Rep.%20Markey.pdf.

[70] William B. Peterson. Letter from General Counsel, Verizon Wireless to Edward J. Markey, U.S. Rep. May 22 2012. markey.house.gov/sites/markey.house.gov/files/documents/Verizon%20Wireless%20Response%20to%20Rep.%20Markey.pdf.

[71] Julian Sanchez. How Shall I Wiretap Thee? Let Me Count the Ways. *CATO @ Liberty*, July 11 2012. www.cato-at-liberty.org/how-shall-i-wiretap-thee-let-me-count-the-ways/.

[72] Rachel Maddow. Interview with Eric Schmidt, Chief Executive Officer, Google, Inc. *FORA.tv*, August 28 2008. www.youtube.com/watch?v=xwq7le9zSv0.

[73] Jared J. Nylund. Fire with Fire: How the FBI Set Technical Standards for the Telecommunications Industry under CALEA. *CommLaw Conspectus*, 8(2):329, 2000.

[74] James X. Dempsey. Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy. *Albany Law Journal of Science & Technology*, 8(1):65, 1997.

[75] James E. Holloway, Elaine Seeman, Margaret O'Hara, and Arno Forst. Regulation and Public Policy in the Full Deployment of the Enhanced Emergency Call System (E-911) and Their Influence on Wireless Cellular and Other Technologies. *Boston University Journal of Science & Technology Law*, 12(1):93, 2006.

[76] Torrentspy. TorrentSpy Privacy Policy. web.archive.org/web/20070410082408/http://www.torrentspy.com/privacy.asp.

[77] Eric Bangeman. Judge: TorrentSpy Must Preserve Data in RAM. *Ars Technica*, August 28 2007. arstechnica.com/tech-policy/news/2007/08/judge-torrentspy-must-preserve-data-in-ram.ars.

[78] The Pirate Bay. Legal Threats. `thepiratebay.org/legal`.

[79] Torrentspy. Torrent Acts to Protect Privacy. `web.archive.org/web/20071219133236/http://www.torrentspy.com./US_Privacy.asp`.

[80] Brian Smith. Email from Chief Technical Officer, Hush Communications Corporation to Kevin Poulsen, Reporter, Wired News. November 5 2007. `web.archive.org/web/20080315230526/http://blog.wired.com/27bstroke6/hushmail-privacy.html`.

[81] Ryan Singel. Encrypted E-Mail Company Hushmail Spills to Feds. *Wired*, November 7 2007. `www.wired.com/threatlevel/2007/11/encrypted-e-mai`.

[82] Albert Gidari. Written Testimony of Partner, Perkins Coie LLP. *Hearing on "Electronic Communications Privacy Act Reform," House Judiciary Committee, Subcommittee on the Constitution, Civil Rights, and Civil Liberties*, May 5 2010. `judiciary.house.gov/hearings/pdf/Gidari100505.pdf`.

[83] Corinna Cortes, Daryl Pregibon, and Chris Volinsky. Communities of Interest. In *Proceedings of the Fourth International Conference on Advances in Intelligent Data Analysis*, pages 105–114, 2001.

[84] Eric Lichtblau. F.B.I. Data Mining Reached Beyond Initial Targets. *The New York Times*, September 9 2007. `www.nytimes.com/2007/09/09/washington/09fbi.html`.

[85] Office of the Inspector General, Department of Justice. A review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records, January 2010. `www.justice.gov/oig/special/s1001r.pdf`.

[86] Tim Shorrock. *Spies for Hire: The Secret World of Intelligence Outsourcing*. Simon & Schuster, 2008.

[87] Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Final Report: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans. page 355, 1976. `www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIIf.htm`.

[88] SEARCH, The National Consortium for Justice Information and Statistics. High-Tech Crime — ISP List, 2012. `www.search.org/programs/hightech/isp`.

[89] Office of the Inspector General, Department of Justice. Findings and Recommendations. *The Implementation of the Communications Assistance for Law Enforcement Act*, March 2006. `www.justice.gov/oig/reports/FBI/a0613/findings.htm`.

[90] James Bamford. The NSA Is Building the Country's Biggest Spy Center (Watch What You Say). *Wired*, March 15 2012. `www.wired.com/threatlevel/2012/03/ff_nsadatacenter/`.

[91] Ryan Singel. Point, Click . . . Eavesdrop: How the FBI Wiretap Net Operates. *Wired*, August 29 2007. `www.wired.com/politics/security/news/2007/08/wiretap`.

[92] Ryan Singel. Secret Data in FBI Wiretapping Audit Revealed With Ctrl+C. *Wired*, May 16 2008. `www.wired.com/threatlevel/2008/05/secret-data-in`.

[93] Kevin Poulsen. Whistle-Blower: Feds Have a Backdoor Into Wireless Carrier — Congress Reacts. *Wired*, March 6 2008. `www.wired.com/threatlevel/2008/03/whistleblower-f/`.

[94] Ellen Nakashima and Dan Eggen. Former CEO Says U.S. Punished Phone Firm.

The Washington Post, October 12 2007. www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202485.html.

[95] James Risen and Eric Lichtblau. Court Affirms Wiretapping Without Warrants. *The New York Times*, January 16 2009. www.nytimes.com/2009/01/16/washington/16fisa.html.

[96] The American Civil Liberties Union. An Open Letter to Wireless Carriers from the ACLU on Location Tracking of Cell Phones. November 9 2011. www.aclu.org/technology-and-liberty/open-letter-wireless-carriers-aclu-location-tracking-cell-phones.

[97] Eric Lichtblau, James Risen, and Scott Shane. Wider Spying Fuels Aid Plan for Telecom Industry. *The New York Times*, December 16 2007. www.nytimes.com/2007/12/16/washington/16nsa.html.

[98] Eric Lichtblau. Congress Strikes Deal to Overhaul Wiretap Law. *The New York Times*, June 20 2008. www.nytimes.com/2008/06/20/washington/20fisa.html.

[99] Mike McConnell. Op-Ed: Help Me Spy on Al Qaeda. *The New York Times*, December 10 2007. www.nytimes.com/2007/12/10/opinion/10mcconnell.html.

[100] Eric Lichtblau. Police Are Using Phone Tracking as a Routine Tool. *The New York Times*, March 31 2012. www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html.

[101] Bob Sullivan. EXCLUSIVE: What local cops learn, and carriers earn, from cellphone records. *The RedTape Chronicles on msnbc.com*, April 18 2012. redtape.msnbc.msn.com/_news/2012/04/18/11252640-exclusive-what-local-cops-learn-and-carriers-earn-from-cellphone-records.

[102] Cox Communications. Notice to parties serving subpoenas on Cox Communications, April 17 2012. ww2.cox.com/aboutus/policies/lea-information.cox.

[103] Robert Morgester. Paying for the production of records in criminal cases. *FIREWALL, The High-Technology Crime Newsletter of the CDAA*, 3(2), July 14 2005.

[104] Office of the Inspector General, Department of Justice. Summary of Findings. *The Federal Bureau of Investigations Management of Confidential Case Funds and Telecommunication Costs*, January 2008. www.justice.gov/oig/reports/FBI/a0803/index.htm.

[105] Interview with Hemanshu Nigam, Chief Security Officer, MySpace, in Washington D.C., February 4 2010.

[106] Facebook. Information for Law Enforcement Authorities. November 28 2011. www.facebook.com/safety/groups/law/guidelines/.

[107] Sonic.net. Notice to Parties Serving Valid Legal Process on Sonic.net, Inc / Sonic Telecom, LLC. 2012. wiki.sonic.net/images/7/70/Sonic.net_Legal_Process_Policy_2012.pdf.

[108] Steven Aftergood. Implementing Domestic Intelligence Surveillance. *Secrecy News*, October 15 2007. www.fas.org/blog/secrecy/2007/10/implementing_domestic_intellig.html.

[109] Verizon Wireless. Law Enforcement Resource Team (Presentation). info.publicintelligence.net/VerizonLawEnforcementResourceTeam.pdf.

[110] Todd S. Schulman. Letter from Assistant General Counsel, Verizon to Arleta D. Cunningham, U.S. Marshals Service. September 14 2009. files.cloudprivacy.net/verizon-price-list-letter.PDF.

[111] Cacciottolo Mario. The Streisand Effect: When censorship backfires. *BBC News*, June 15 2012. www.bbc.co.uk/news/uk-18458567.

[112] Ryan Singel. Whistleblower Site Back After Microsoft Withdraws Complaint. *Wired*, February 25 2010. www.wired.com/threatlevel/2010/02/microsoft-withdraws-cryptome-complaint.

[113] Senate Select Committee on Intelligence. Committee Report: Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2007. page 9, October 26 2007. www.gpo.gov/fdsys/pkg/CRPT-110srpt209/pdf/CRPT-110srpt209.pdf.

[114] Dan Boneh. The Difficulties of Tracing Spam. *Report to the Federal Trade Commission*, September 9 2004. www.ftc.gov/reports/rewardsys/expertrpt_boneh.pdf.

[115] Google. Seeing a Sender's IP Address. *Security and privacy policies*, September 21 2011. support.google.com/mail/bin/answer.py?hl=en&answer=26903.

[116] Joseph Kahn. Yahoo helped chinese to prosecute journalist. *The New York Times*, September 8 2005. www.nytimes.com/2005/09/07/business/worldbusiness/07iht-yahoo.html.

[117] Brad Stone. Concern for Those Who Screen the Web for Barbarity. *The New York Times*, July 19 2010. www.nytimes.com/2010/07/19/technology/19screen.html.

[118] Christopher Soghoian. Editorial: It's Time for a Child Porn Czar. *Surveillance State*, December 9 2008. news.cnet.com/8301-13739_3-10118923-46.html.

[119] Miles Benson. In the Name of Homeland Security, Telecom Firms are Deluged with Subpoenas. *Global Research*, December 30 2005. www.globalresearch.ca/index.php?context=va&aid=1677.

[120] New York State Office of the Attorney General. Attorney General Cuomo Announces Additional Social Networking Sites Join His Initiative To Eliminate

Sharing Of Thousands Of Images Of Child Pornography, June 29 2010. www.ag.ny.gov/press-release/attorney-general-cuomo-announces-additional-social-networking-sites-join-his.

[121] Joeseph Menn. Social networks scan for sexual predators, with uneven results. *Reuters*, July 12 2012. www.reuters.com/article/2012/07/12/us-usa-internet-predators-idUSBRE86B05G20120712.

[122] U.S. House of Representatives. House Report: Communications Assistance for Law Enforcement Act. page 25, October 14 1994. www.askcalea.net/docs/hr103827.pdf.

[123] Paul Ohm. The Rise and Fall of Invasive ISP Surveillance. *University of Illinois Law Review*, 2009:1417, 2009.

[124] Jacob Appelbaum et al. Open letter to Eric Schmidt, Chief Executive Officer, Google, Inc., June 16. www.cloudprivacy.net/letter.

[125] Ariel Rideout. Making security easier. *Official Gmail Blog*, July 24 2008. gmailblog.blogspot.com/2008/07/making-security-easier.html.

[126] Adam Langley. Overclocking SSL. *ImperialViolet (Blog)*, June 25 2010. www.imperialviolet.org/2010/06/25/overclocking-ssl.html.

[127] Andrew Jacobs and Miguel Helft. Google, citing attack, threatens to exit china. *The New York Times*, January 12 2010. www.nytimes.com/2010/01/13/world/asia/13beijing.html.

[128] Sam Schillace. Default HTTPS Access for Gmail. *Official Gmail Blog*, January 12 2010. gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html.

[129] Evan Roseman. Search More Securely with Encrypted Google Web Search. *Google Official Blog*, June 25 2010. `googleblog.blogspot.com/2010/05/search-more-securely-with-encrypted.html`.

[130] Evelyn Kao. Making search more secure. *Google Official Blog*, October 18 2011. `googleblog.blogspot.com/2011/10/making-search-more-secure.html`.

[131] Sid Stamm. Rolling Out HTTPS Google search. *Mozilla Privacy Blog*, May 7 2012. `blog.mozilla.org/privacy/2012/05/07/rolling-out-https-google-search/`.

[132] Mike Perry. Automated HTTPS Cookie Hijacking. August 14 2008. `fscked.org/blog/fully-automated-active-https-cookie-hijacking`.

[133] Moxie Marlinspike. SSLStrip. `www.thoughtcrime.org/software/sslstrip`.

[134] Kate Murphy. New hacking tools pose bigger threats to Wi-Fi users. *The New York Times*, February 17 2011. `www.nytimes.com/2011/02/17/technology/personaltech/17basics.html`.

[135] Lance Whitney. Senator wants more secure Web sites for Wi-Fi use. *CNET News*, February 29 2011. `news.cnet.com/8301-1009_3-20037253-83.html`.

[136] Pamela Jones Harbour. Remarks Before Third Federal Trade Commission Exploring Privacy Roundtable in Washington, D.C., March 17 2010. `www.ftc.gov/speeches/harbour/100317privacyroundtable.pdf`.

[137] Dick Cradock. Hotmail Security Improves with Full-Session HTTPS Encryption. *Inside Windows Live*, November 9 2010. `windowsteamblog.com/windows_live/b/windowslive/archive/2010/11/09/hotmail-security-improves-with-full-session-https-encryption.aspx`.

[138] Alex Rice. A Continued Commitment to Security. *The Facebook Blog*, January 26 2011. www.facebook.com/blog.php?post=486790652130.

[139] Twitter. Making Twitter more secure: HTTPS. *twitter blog*, March 15 2011. blog.twitter.com/2011/03/making-twitter-more-secure-https.html.

[140] Twitter. Securing your Twitter experience with HTTPS. *twitter blog*, February 13 2012. blog.twitter.com/2012/02/securing-your-twitter-experience-with.html.

[141] Mozilla. Keep your Firefox in Sync. www.mozilla.org/en-US/mobile/sync/.

[142] Mozilla. Weave. January 24 2008. wiki.mozilla.org/Labs/Weave/OAuth.

[143] SpiderOak. Does SpiderOak use encryption when storing and transferring data? *Frequently Asked Questions*. spideroak.com/faq/questions/3/does_spideroak_use_encryption_when_storing_and_transferring_data.

[144] Wuala. Security. wuala.com/en/learn/technology.

[145] Tarsnap (home page). www.tarsnap.com.

[146] Drew Houston and Arash Ferdowsi. Privacy, Security & Your Dropbox (Updated). *The Dropbox Blog*, May 16 2011. blog.dropbox.com/?p=735.

[147] Christopher Soghoian. Two honest Google employees: our products don't protect your privacy. *Slight Paranoia (Blog)*, November 2 2011. paranoia.dubfire.net/2011/11/two-honest-google-employees-our.html.

[148] Christopher Soghoian. Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era. *Journal on Telecommunications & High Technology Law*, 8:359, 2010.

[149] Robert Siegel. Interview with Eric Schmidt, CEO, Google. *All Things Considered*, October 2 2009. www.npr.org/2009/10/02/113450803/ceo-google-knows-a-lot-about-you-then-forgets.

[150] Brad Stone. Microsoft offers privacy options for its search engine. *The New York Times*, July 23 2007. www.nytimes.com/2007/07/23/technology/23microsoftweb.html.

[151] Kevin Bankston. From EFF's Secret Files: Anatomy of a Bogus Subpoena. *Electronic Frontier Foundation Deeplinks Blog*, November 9 2009. www.eff.org/deeplinks/2009/11/effs-secret-files-anatomy-bogus-subpoena.

[152] Ryan Singel. Google To Anonymize Data — Updated. *Wired*, March 14 2007. www.wired.com/threatlevel/2007/03/google_to_anony.

[153] Peter Fleischer, Jane Horvath, and Alma Whitten. Another Step to Protect User Privacy. *Google Official Blog*, September 8 2008. googleblog.blogspot.com/2008/09/another-step-to-protect-user-privacy.html.

[154] Declan McCullagh. FBI: New Internet addresses could hinder police investigations. *CNET News*, May 31 2012. news.cnet.com/8301-1009_3-57445157-83.

[155] T-Mobile. T-Mobile Enables IPv6 Across Nationwide Mobile Network. *Issues & Insights Blog*, June 5 2012. blog.t-mobile.com/2012/06/05/t-mobile-enables-ipv6-across-nationwide-mobile-network-5.

[156] Time Warner Cable. Subpoena Instructions. May 4 2012. www.timewarnercable.com/corporate/subpoenacompliance.html.

[157] Alain Durand et al. Logging Recommendations for Internet-Facing Servers. RFC 6302, RFC Editor, June 2011. www.rfc-editor.org/info/rfc6302.

[158] Twitter. Guidelines for Law Enforcement. 2012. support.twitter.com/articles/41949-guidelines-for-law-enforcement.

[159] Dropbox. Law Enforcement Handbook. 2012. dl.dropbox.com/s/77fr4t57t9g8tbo/law_enforcement_handbook.html.

[160] LinkedIn. Law Enforcement Data Request Guidelines. 2012. help.linkedin.com/ci/fattach/get/1568450/0/filename/LinkedIn%20Law%20Enforcement%20Data%20Request%20Guidelines.pdf.

[161] David Kravets. Which Telecoms Store Your Data the Longest? Secret Memo Tells All. *Wired*, September 28 2011. www.wired.com/threatlevel/2011/09/cellular-customer-data/.

[162] Federal Bureau of Investigation. FY 2008 Authorization and Budget Request to Congress. pages 4–19,4–20. www.fas.org/irp/agency/doj/fbi/2008just.pdf.

[163] MySpace.com. Law Enforcement Investigators Guide. June 23 2006. cryptome.org/isp-spy/myspace-spy.pdf.

[164] MySpace.com. Law Enforcement Guide. November 1 2007. info.publicintelligence.net/MySpaceLawEnforcementGuide2007.pdf.

[165] Facebook. Subpoena / Search Warrant Guidance. February 2007. info.publicintelligence.net/Facebook2007.pdf.

[166] Facebook. Subpoena / Search Warrant Guidelines. February 2008. info.publicintelligence.net/Facebook2008.pdf.

[167] Department of Justice. Searching and Seizing Computers and Obtaining Electronic Evidence Manual, September 2009. www.justice.gov/criminal/cybercrime/ssmanual/03ssma.html.

[168] Marc J. Zwillinger and Christian S. Genetski. Criminal Discovery of Internet Communications under the Stored Communications Act: It's Not a Level Playing Field. *Journal of Criminal Law and Criminology*, page 569, 2006.

[169] Bureau of Justice Assistance. The ECPA, ISPs & Obtaining E-mail: A Primer for Local Prosecutors, July 2005. www.ndaa.org/pdf/ecpa_isps_obtaining_email_05.pdf.

[170] David Kravets. Yahoo Beats Feds in E-Mail Privacy Battle. *Wired*, April 16 2010. www.wired.com/threatlevel/2010/04/emailprivacy-2.

[171] U.S. Internet Service Provider Association. Electronic Evidence Compliance - A Guide for Internet Service Providers. *Berkeley Technology Law Journal*, 18:945, 2003.

[172] Mike Duffy. Email from Special Agent, Florida Department of Law Enforcement to Internet Crimes Against Children Task Force Email List. June 26 2009. file.wikileaks.info/leak/myspace-yahoo-att-2009.txt.

[173] Memorandum in Support of Verizon's Motion to Dismiss Plaintiff's Master Consolidated Complaint at 27, *In re National Security Agency Telecommunications Records Litigation*, 700 F. Supp. 2d 1182 (N.D. Cal. 2010) (MDL No. 06-1791 VRW).

[174] Paul Sonne. U.S. Asks Twitter for WikiLeaks Data. *Wall Street Journal*, January 10 2011. online.wsj.com/article/SB10001424052748704482704576072081788251562.html.

[175] Charlie Savage. WikiLeaks Allies Fight Order on Twitter Data. *The New York Times*, February 15 2011. www.nytimes.com/2011/02/16/world/16wikileaks.html.

[176] Julia Angwin. Secret Orders Target Email. *Wall Street Journal*, October 9 2011. online.wsj.com/article/SB10001424052970203476804576613284007315072.html.

[177] Milton J. Valencia. Occupy blogger fighting subpoena. *The Boston Globe*, December 29 2011. articles.boston.com/2011-12-29/metro/30565674_1_twitter-users-subpoena-hashtags.

[178] Brian D. Kaiser. Government Access to Transactional Information and the Lack of Subscriber Notice. *Boston University Journal of Science & Technology Law*, 8:648, 2002.

[179] SpiderOak. Privacy Policy. May 1 2011. spideroak.com/privacy_policy.

[180] Marcia Hofmann, Rainey Reitman, and Cindy Cohn. 2012: When the Government Comes Knocking, Who Has Your Back? *Electronic Frontier Foundation*, May 31 2012. www.eff.org/sites/default/files/who-has-your-back-2012_0.pdf.

[181] Michael D. Hintze. Statement of Associate General Counsel, Microsoft. *Hearing on "ECPA Reform and the Revolution in Cloud Computing," House Judiciary Committee, Subcommittee on the Constitution, Civil Rights, and Civil Liberties*, page 73, September 23 2010. judiciary.house.gov/hearings/printers/111th/111-149_58409.PDF.

[182] Richard Salgado. Written Testimony of Senior Counsel, Law Enforcement and Information Security, Google Inc. *Hearing on "ECPA and the Cloud," House Judiciary Committee, Subcommittee on the Constitution, Civil Rights, and Civil Liberties*, September 23 2010. static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/googleblogs/pdfs/google_testimony_rick_salgado.pdf.

[183] Richard Salgado. Regulating the Cloud. *Big Brother in the 21st Century? Reforming*

the Electronic Communications Privacy Act, University of San Francisco Law Review Symposium, February 24 2012. www.youtube.com/watch?v=MCuAf0kE-1g.

[184] Kevin Bankston. EXCLUSIVE: Google Takes a Stand for Location Privacy, Along with Loopt. *Electronic Frontier Foundation Deeplinks Blog*, March 4 2009. www.eff.org/deeplinks/2009/03/exclusive-google-takes-stand-location-privacy-alon.

[185] Kenneth A. Bamberger and Deirde K. Mulligan. Privacy on the Books and on the Ground. *Stanford Law Review*, 63:247, January 2011.

[186] E.B. Boyd. Google Privacy Chief: 'We Absolutely Compete on Privacy'. *BayNewser*, January 29 2010. web.archive.org/web/20100202160618/http://www.mediabistro.com/baynewser/privacy/google_privacy_chief_we_absolutely_compete_on_privacy_150406.asp.

[187] Katherine Mangu-Ward. Search Engines Compete on Privacy. *Reason*, August 13 2007. reason.com/blog/2007/08/13/search-engines-compete-on-priv.

[188] Julia Angwin. Microsoft's "Do Not Track" Move Angers Advertising Industry. *Wall Street Journal*, May 31 2012. blogs.wsj.com/digits/2012/05/31/microsofts-do-not-track-move-angers-advertising-industry.

[189] Google. FAQ. *Policies & Principles — FAQ*. www.google.com/privacy_faq.html.

[190] Google. Google's Privacy Principles. *YouTube video*, January 26 2010. www.youtube.com/watch?v=5fvL3mNtl1g.

[191] Ina Fried. Microsoft Probes Possible Privacy Snafu. *CNET News*, February 16 2010. news.cnet.com/8301-13860_3-10454741-56.html.

[192] Jun Yan et al. How much can Behavioral Targeting Help Online Advertising? In *Proceedings of the 18th international conference on World Wide Web*, WWW '09, pages 261–270, 2009.

[193] Christopher Soghoian. The Problem of Anonymous Vanity Searches. *I/S: A Journal of Law and Policy for the Information Society*, 3:299, 2007.

[194] Saikat Guha, Bin Cheng, and Paul Francis. Privad: Practical Privacy in Online Advertising. In *Proceedings of the 8th Symposium on Networked Systems Design and Implementation (NSDI)*, Boston, MA, Mar 2011.

[195] Mikhail Bilenko and Matthew Richardson. Predictive client-side profiles for personalized advertising. In *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining*, KDD '11, pages 413–421, New York, NY, USA, 2011. ACM.

[196] Vincent Toubiana, Arvind Narayanan, Dan Boneh, Helen Nissenbaum, and Solon Barocas. Adnostic: Privacy preserving targeted advertising. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2010, San Diego, California, USA, 28th February - 3rd March 2010*. The Internet Society, 2010.

[197] Albert Gidari. Designing The Right Wiretap Solution: Setting Standards Under CALEA. *IEEE Security & Privacy*, 4(3):29–36, June 2006.

[198] James Risen and Eric Lichtblau. Bush Lets U.S. Spy on Callers Without Courts. *The New York Times*, December 16 2005.
`www.nytimes.com/2005/12/16/politics/16program.html`.

[199] David Kernohan. Misattributing Cyber-Lawyers, Wilde on Twitter and a TINA turn - Free Culture and Value. *The Followers Of The Apocalypse (Blog)*, September 20 2011.

followersoftheapocalyp.se/misattributing-cyber-lawyers-wilde-on-twitter.

[200] Bianca Bosker. Al Franken Warns Facebook, Google Users: 'You Are Their Product'. *The Huffington Post*, March 30 2012. www.huffingtonpost.com/2012/03/30/al-franken-privacy-facebook-google_n_1392442.html.

[201] Louise Story and Brad Stone. Facebook Retreats on Online Tracking. *The New York Times*, November 30 2007. www.nytimes.com/2007/11/30/technology/30face.html.

[202] Julia Angwin and Jennifer Valentino-Devries. Google's iPhone Tracking. *Wall Street Journal*, February 17 2012. online.wsj.com/article/SB10001424052970204880404577225380456599176.html.

[203] Miguel Helft. Critics Say Google Invades Privacy With New Service. *The New York Times*, February 12 2010. www.nytimes.com/2010/02/13/technology/internet/13google.html.

[204] Julia Angwin. Congressmen Seek Answers to 'Supercookies'. *Wall Street Journal*, September 27 2011. blogs.wsj.com/digits/2011/09/27/congressmen-seek-answers-to-supercookies.

[205] Jennifer Valentino-Devries. Lawmakers Target Google's Tracking. *Wall Street Journal*, February 18 2012. online.wsj.com/article/SB10001424052970204059804577229681587016516.html.

[206] Julia Angwin. Apple, Google Take Heat. *Wall Street Journal*, May 10 2011. online.wsj.com/article/SB10001424052748703730804576315121174761088.html.

[207] Julia Angwin and Amir Efrati. Google Settles With FTC Over Google Buzz. *Wall*

Street Journal, 30 2011. online.wsj.com/article/SB10001424052748703806304576232600483636490.html.

[208] Shayndi Raice and Julia Angwin. Facebook 'Unfair' on Privacy. *Wall Street Journal*, November 30 2011. online.wsj.com/article/SB10001424052970203441704577068400622644374.html.

[209] Edward Wyatt. U.S. Penalizes Online Company in Sale of Personal Data. *The New York Times*, June 12 2012. www.nytimes.com/2012/06/13/technology/ftc-levies-first-fine-over-internet-data.html.

[210] Jessica E. Vascellaro. Facebook Settles Class-Action Suit Over Beacon Service. *Wall Street Journal*, September 18 2009. online.wsj.com/article/SB125332446004624573.html.

[211] Jennifer Valentino-Devries and Emily Steel. 'Cookies' Cause Bitter Backlash. *Wall Street Journal*, September 19 2010. online.wsj.com/article/SB10001424052748704416904575502261335698370.html.

[212] Yukari Iwatani Kane. Apple Sued Over Mobile App Privacy. *Wall Street Journal*, December 28 2010. blogs.wsj.com/digits/2010/12/28/apple-sued-over-mobile-app-privacy.

[213] Stewart Baker. Statement of Partner, Steptoe & Johnson. *Hearing on "Fourth Amendment And The Internet," House Judiciary Committee, Subcommittee on the Constitution*, page 135, April 6 2000. commdocs.house.gov/committees/judiciary/hju66503.000/hju66503_0f.htm.

[214] Geoffrey A. Fowler, Devlin Barrett, and Sam Schechner. U.S. Shuts Offshore File-Share 'Locker'. *Wall Street Journal*, January 20 2012. online.wsj.com/article/SB10001424052970204616504577171060611948408.html.

[215] James A. Baker. Written Testimony of Associate Deputy Attorney General, Department of Justice. *Hearing on "The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age," Senate Judiciary Committee*, April 6 2011. www.judiciary.senate.gov/pdf/11-4-6%20Baker%20Testimony.pdf.

[216] Julian Sanchez. The Strange Case Against ECPA Reform. *CATO @ Liberty*, April 11 2011. www.cato-at-liberty.org/the-strange-case-against-ecpa-reform.

[217] Declan McCullagh. House panel approves broadened ISP snooping bill. *CNET News*, July 28 2011. news.cnet.com/8301-31921_3-20084939-281.

[218] Howard Beales, Richard Craswell, and Steven C. Salop. The Efficient Regulation of Consumer Information. *Journal of Law & Economics*, 24:491, 1981.

[219] Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. Emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, 2007.

[220] Xavier Gabaix and David Laibson. Shrouded Attributes, Consumer Myopia, and Information Suppression in Competitive Markets. *The Quarterly Journal of Economics*, 121(2):505–540, May 2006.

[221] Jim Dempsey. California Adopts Smart Grid Privacy Rule. *Center for Democracy & Technology Blog*, August 16 2011. www.cdt.org/blogs/jim-dempsey/168california-adopts-smart-grid-privacy-rule.

[222] Kevin S. Bankston. Only The DOJ Knows: The Secret Law of Electronic Surveillance. *University of San Francisco Law Review*, 41(4):559, 2007.

[223] Charlie Savage. Senators Say Patriot Act Is Being Misinterpreted. *The New York Times*, May 26 2011. www.nytimes.com/2011/05/27/us/27patriot.html.

[224] Charlie Savage. Democratic Senators Issue Strong Warning About Use of the Patriot Act. *The New York Times*, March 16 2012. www.nytimes.com/2012/03/16/us/politics/democratic-senators-warn-about-use-of-patriot-act.html.