Minnesota Journal of Law, Science & Technology

Volume 12 | Issue 1 Article 8

2011

An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government

Christopher Soghoian

Soghoian C. An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government. *Minnesota Journal of Law, Science & Technology*. 2011;12(1):191-237.

An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government

Christopher Soghoian*

I. INTRODUCTION: HOW DO COMPANIES PROTECT THEIR CUSTOMERS' PRIVACY?

> "Verizon has a longstanding and vigorous commitment to protecting its customers' privacy and takes comprehensive steps to protect that privacy."[1]
>
> "At Verizon, privacy is a key priority. We know that consumers will use the full capabilities of our communications networks only if they trust that their information will remain private."[2]
>
> "At Google, we are keenly aware of the trust our users place in us, and our responsibility to protect their privacy."[3]

---

* Graduate Fellow, Center for Applied Cybersecurity Research, Indiana University. Ph.D. Candidate, School of Informatics and Computing, Indiana University. Email: chris@soghoian.net. Other research papers available at http://www.dubfire.net. This article has been written in my capacity as an academic researcher. Some material contained within was obtained through original investigative reporting. As such, this work should be considered a scholarly publication as well as legitimate journalism. The opinions expressed within and any errors are my own. Thanks to Kevin Bankston, Al Gidari, Jennifer Granick, Paul Ohm, Julian Sanchez, Joris Van Hoboken, as well as several anonymous individuals for their assistance and feedback on the theories presented in this article.

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

2. Ivan Seidenberg, *A Message from Verizon's Chief Executive Officer*, VERIZON, http://www22.verizon.com/about/privacy/letter/ (last visited Oct. 13, 2010).

3. *Privacy FAQs*, GOOGLE, http://www.google.com/privacy_faq.html (last

> "Google values our users' privacy first and foremost. Trust is the basis of everything we do, so we want you to be familiar and comfortable with the integrity and care we give your personal data."[4]

> "Microsoft takes customers' privacy seriously . . . ."[5]

> "At Microsoft, we believe individuals should control the use of their personal information online, and should be free from fear that their personal and financial data will be stolen or used by others without their consent."[6]

Across corporate America, companies have come to recognize the importance of privacy. Practically every corporate website has a privacy policy,[7] and the majority of Fortune 500 companies have appointed Chief Privacy Officers.[8] In statements to consumers and the press, most companies pledge to value, respect, and fight for their customers' privacy. Some companies even claim to compete on privacy;[9] most visibly, the major search engines that have repeatedly one-upped each other, adopting ever-more privacy-protecting data retention policies.[10]

---

visited Sept. 26, 2010).

4. Marissa Mayer, *What Comes Next in This Series? 13, 33, 53, 61, 37, 28…*, OFFICIAL GOOGLE BLOG (July 3, 2008, 1:36 PM), http://googleblog.blogspot.com/2008/07/what-comes-next-in-this-series-13-33-53.html.

5. Ina Fried, *Microsoft Probes Possible Privacy Snafu*, CNET NEWS, (Feb. 16, 2010, 5:40 PM), http://news.cnet.com/8301-13860_3-10454741-56.html?tag=contentMain;contentBody;1n.

6. Microsoft and Privacy, MICROSOFT (Sep. 2009), http://go.microsoft.com/?linkid=9688090

7. This is likely because of California's Online Privacy Protection Act of 2003. CAL. BUS. & PROF. CODE §§ 22575–22579 (Deering 2010) ("An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site.").

8. *See* Kenneth A. Bamberger & Deirde K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. (forthcoming Jan. 2011) (manuscript at 2).

9. *E.g.*, E.B. Boyd, *Google Privacy Chief: 'We Absolutely Compete on Privacy,'* BAYNEWSER (Jan. 29, 2010, 3:17 AM), http://www.mediabistro.com/baynewser/privacy/google_privacy_chief_we_absolutely_compete_on_privacy_150406.asp).

10. *See* Richard Koman, *Search Engines Compete for Privacy Bragging Rights*, NEWSFACTOR.COM (July 24, 2007, 11:53 AM), http://www.newsfactor.com/story.xhtml?story_id=010000TXY69E&full_skip=1 ("After years of insisting that they should be trusted to keep users' search

When companies argue that they take privacy seriously, compete on privacy, or are transparent about their privacy practices, what they are usually talking about is one limited aspect of privacy. That is, they are discussing their own collection and commercial use of customer data and the extent to which they share it with other companies. This is often motivated by a desire to avoid the ire of government regulators such as the U.S. Federal Trade Commission (FTC) and the European Article 29 Working Party.[11]

Privacy is a bigger issue than the commercial use of data. Specifically, most firms are often unwilling to discuss the privacy threat posed by law enforcement and intelligence agencies' access to their customers' data or the degree to which they proactively assist, or resist, such access. Few companies effectively protect their customers' data from intrusive government searches. Furthermore, in many cases, telecommunications carriers and Internet service providers (ISPs) that have repeatedly pledged to protect user privacy go out of their way to actively assist and facilitate government access to their customers' most private information.

For example, even though Verizon has a "longstanding and vigorous commitment to protecting its customers' privacy,"[12] the company has argued in court that it has a First Amendment right to voluntarily provide information about its customers' private communications to the National Security Agency.[13] This may be a valid legal argument, but it is not the kind of position that a company that has pledged to protect users' privacy should take. Certainly, it is not an official position that the company advertises to its customers on its website or in its privacy policy.

---

histories indefinitely, search engines are suddenly competing to limit data retention."); Katherine Mangu-Ward, *Search Engines Compete on Privacy*, REASON (Aug. 13, 2007), http://reason.com/blog/2007/08/13/search-engines-compete-on-priv ("Search engines are in an arms race to offer better privacy protections to the users . . . ."); Joseph Weisenthal, *Search Engines Compete on Accuracy, Privacy Policies*, TECHDIRT (July 23, 2007, 3:45 PM), http://techdirt.com/articles/20070723/100944.shtml ("With Google taking some hits over its data retention practices, its competitors are hoping that they can use the privacy issue to their advantage.").

11. *See generally* Bamberger, *supra* note 8, at 23.

12. Milch, *supra* note 1, at 1.

13. Memorandum in Support of Verizon's Motion to Dismiss Plaintiff's Master Consolidated Complaint at 27, *In re* Nat'l Sec. Agency Telecomm. Records Litig., 700 F. Supp. 2d 1182 (N.D. Cal. 2010) (MDL No. 06-1791 VRW).

Google has made bold statements about the "trust our users place in us, and our responsibility to protect that privacy."[14] The company also has a YouTube privacy channel with nearly 50 videos describing the privacy features built into its products and one that promises that the company "makes privacy a priority in everything we do."[15] Absent from the company's YouTube privacy channel, however, is a disclosure that one of the main reasons the company retains identifying user log data is so that it may deliver it to the government.[16]

Finally, Microsoft has pledged that it takes its "customers' privacy seriously."[17] However, when asked by the New York Times if the company was considering a policy to log no search data at all, Peter Cullen, Microsoft's chief privacy strategist, argued that too much privacy was actually 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."[18] Information about the company's commitment to maintaining such a "balance" by storing user data in order to later make it available to law enforcement agencies is nowhere to be found in the company's privacy policy or anywhere else on the company's website.

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

14. *Privacy FAQs*, *supra* note 3.

15. googleprivacy, *Google's Privacy Principles*, YOUTUBE (Jan. 26, 2010), http://www.youtube.com/watch?v=5fvL3mNtl1g.

16. *See* Interview by Robert Siegel with Eric Schmidt, CEO, Google, on NPR (Oct. 2, 2009), *available at* http://www.npr.org/templates/story/story.php?storyId=113450803 ("[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.").

17. Fried, *supra* note 5.

18. Brad Stone, *Microsoft Offers Privacy Options for Its Search Engine*, N.Y. TIMES, July 23, 2007, *available at* http://www.nytimes.com/2007/07/23/technology/23microsoftweb.html.

This is not to say that Microsoft, Google, and Verizon are hostile to user privacy—merely that when these and other firms speak about their commitment to protecting their customers' privacy, what they really mean is that they will protect their customers' data from improper access or use by commercial entities. The fact that these firms have a limited definition of privacy is not made clear to consumers, who may mistakenly believe that the companies to whom they entrust their data are committed to protecting their privacy from all threats, and not just those from the private sector.

While most firms 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 they retain users' private data—rather, they rarely discuss these differences and never compete on them. This article aims to shed light upon these rather important privacy differences among service providers, both technical and legal, which impact the extent to which government agencies can obtain users' private data.

Section II of this article will explore the numerous ways in which the technical design and implementation details of companies' applications and networks can assist or frustrate government access to their customers' data. While some firms have adopted technologies and policies that are significantly more privacy preserving than their competitors, few firms will publicly acknowledge or advertise these technical differences, making it almost impossible for consumers to pick a provider based on the degree to which their information is protected and retained.

Section III delves into the Electronic Communications Privacy Act (ECPA) and, in particular, the ways in which a few companies have adopted aggressively pro-privacy interpretations of this federal law, limiting the extent to which government agencies can obtain user data without a court order. Again, just as with their engineering practices, few companies are willing to disclose their interpretations of ECPA or the extent to which they are willing to fight the government. This section sheds significant light on this subject and reveals several novel, privacy-preserving interpretations of ECPA that some service providers have adopted.

Finally, Section IV seeks to address the problems that plague the market. Simply put, firms are not willing to reveal the extent to which they can and do disclose user data to the

government or the engineering and legal policies they have adopted that can effectively limit the government's access to that data. Currently, there is little pressure to compete in this way. This section will propose several ways to fix this fundamentally broken market.

II. RESTRICTING GOVERNMENT ACCESS TO DATA

Technology firms in the United States are largely free to design their products and networks in any way they wish, at least with regard to the extent to which privacy enhancing technologies are included.[19] Outside of the financial and common carrier telephone industries,[20] there are no data retention laws. The few regulations that are applied focus on making sure that companies sufficiently protect their customers' data from improper access by rogue insiders, hackers, and other criminals.

Email, search engine, and broadband ISPs are free to deploy any privacy enhancing technology or policy that they wish to use, even if it may impact or thwart the ability of law enforcement and intelligence agencies to engage in legitimate investigations. Thus, a provider's decision to adopt a particular privacy enhancing technology or to adopt a zero data log retention policy can significantly impact their customers' privacy and freedom. That is, even though a company can be legally compelled to deliver any data in its possession, if the data is encrypted with a key not known to the company—or has not been retained in the first place—the firm will have nothing

19. H.R. REP. NO. 103-827, pt. 1, at 13, 19 (1994) (quoting United States v. New York Tel., 434 U.S. 159, 177 (1977)) ("While the Supreme Court has read [18 U.S.C. 2518(4)] as requiring the Federal courts to compel, upon request of the government, 'any assistance necessary to accomplish an electronic interception,' the question of whether companies have any obligation to design their systems such that they do not impede law enforcement interception has never been adjudicated. . . . [The Communications Assistance for Law Enforcement Act] expressly provides that law enforcement may not dictate system design features and may not bar introduction of new features and technologies.").

20. 47 C.F.R. § 42.6 (2009) ("Each carrier that offers or bills toll telephone service shall retain for a period of 18 months such records as are necessary to provide the following billing information about telephone toll calls: the name, address, and telephone number of the caller, telephone number called, date, time and length of the call. Each carrier shall retain this information for toll calls that it bills whether it is billing its own toll service customers for toll calls or billing customers for another carrier.").

to deliver to the government.

This section will explore several ways that companies' engineering design decisions and data storage policies differ and will analyze the impact that such decisions have on customer privacy. In particular, although most firms do not publicly discuss or compete on the privacy provided by their products, the differences are significant enough that users of one service are often far better protected from government access to their data than users of other providers.

A. LEAKING IP ADDRESSES IN E-MAIL HEADERS

Several of the big free web mail providers intentionally leak their users' IP addresses to anyone that their subscribers contact by email. This engineering decision, something not required by technical standards or law, may offer some benefit for service providers wishing to limit the use of their systems to send unsolicited "spam" email. However, the engineering decision also impacts end users' privacy since users' IP addresses are considered by many to be private information that can be linked to an individual and, potentially, their geographic location—a view shared by both the European Union Article 29 Working Party and the current FTC Chairman.[21]

When a user of Microsoft's Hotmail or Yahoo! Mail services sends an email message to another person, both companies insert the user's actual IP address (that is, the IP address of the computer with which the user is accessing the Microsoft or Yahoo! website) into a header in the email message. While this header is typically not displayed to recipients by most email clients, technically savvy users (such as government investigators) can easily view the full header accompanying an email message to see the originating IP address.

Microsoft's Hotmail system appends the following header to all outgoing emails:

X-Originating-IP: [68.48.136.114][22]

---

21. Interview by Bob Garfield with Jon Leibowitz, Chairman, FTC, on On the Media (Apr. 23, 2010), http://www.onthemedia.org/transcripts/2010/04/23/05 ("[T]here's a question about whether if you can track something back to someone's IP address it's almost the same as personal information. I kind of think it is.").

22. *See* Dan Boneh, Report to the Federal Trade Commission, The Difficulties of Tracing Spam (Sept. 9, 2004),

Yahoo's mail system appends a similar header to all outgoing emails:

> Received: from [68.48.136.114] by web46311.mail.sp1.yahoo.com via HTTP

When Google launched its own free email service, it opted to keep its customers' IP address information private. The company's website confirms this decision and reveals that privacy was one of the factors in not voluntarily appending the IP address to users' outgoing emails:

> IP addresses can be considered sensitive information. As such, Gmail may hide sender IP address information from outgoing mail headers in some circumstances.
>
> Don't worry—we aren't enabling spammers to abuse the system by not revealing IP addresses. Gmail uses many innovative spam filtering mechanisms to ensure that spammers have a difficult time sending bulk emails that arrive in users inboxes.[23]

Facebook appears to have not followed Google's lead, and instead, adopted a policy similar to Microsoft and Yahoo, albeit in a way that is slightly obfuscated.

Going at least as far back as 2006, when a Facebook user commented on another user's profile, left a comment on his "wall," or did any other action that triggered an email notification, the company would provide the IP address of the user initiating the action in the header of the email sent to the recipient of the notification:

> Received: from zuckmail ([68.48.136.114]) by hs.facebook.com with HTTP (ZuckMail).[24]

At some point in 2009, Facebook modified this header slightly, so that the user's IP address was obfuscated via Base64 encoding, which can be trivially reversed with off the shelf tools:

---

http://www.ftc.gov/reports/rewardsys/expertrpt_boneh.pdf. ("These services [Hotmail and Yahoo] embed an X-Originating-IP header in every email they send which completely identifies the sender's network address.")

23. *Seeing a Sender's IP Address*, GOOGLE, https://mail.google.com/support/bin/answer.py?hl=en&answer=26903 (last updated Oct. 11, 2010).

24. *See* Ron Collings, Comment to *Thread: 7.0.1 Beta GWIA Outbound Mail Scrambling HTML Content of Multiplemessages and Adding Multiple Disclaimers - Bug Report*, NOVELL, http://forums.novell.com/novell-product-support-forums/groupwise/groupwise-7x/gw7-gwia/103615-7-0-1-beta-gwia-outbound-mail-scrambling-html-content-multiplemessages-adding-multiple-disclaimers-bug-report.html (Apr. 5, 2006, 6:28 AM)); *Facebook Notifications Leaking Information*, THE CLASSICALLY FORBIDDEN REGION (Dec. 5, 2007, 2:46 AM), http://supersat.livejournal.com/71945.html.

> X-Facebook: from zuckmail ([NjguNDguMTM2LjExNA==]) by www.facebook.com with HTTP (ZuckMail).[25]

News of Facebook's IP address header spread across several popular Internet blogs and forums in May 2010. In response, the company quickly changed the header format so that the user's real IP address was no longer leaked.[26]

The engineering decision to voluntarily provide a user's IP address to the recipients of emails can have a major impact on an end user's privacy and the ability of governments (particularly foreign governments) to investigate them, and can increase or reduce the workload for a service provider.

For example, in the event that a Yahoo! or Hotmail account is used to send an email message that is later deemed to be relevant to an investigation by a U.S. law enforcement agency, the investigators will not need to send Yahoo! or Microsoft a subpoena for the IP address connection logs, but will simply look through the email header and then go directly to the broadband ISP responsible for that IP address. That is, by providing this IP address information in the header of every outgoing email, Yahoo!, Microsoft (and until recently, Facebook) significantly reduced the need for law enforcement to contact them to get user data.

Had Yahoo! or Microsoft not proactively disclosed the IP address information in the header, law enforcement investigators would have had 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 have given the email service providers the opportunity to give their customer notice that his or her records were subpoenaed or to force the police to seek a court order if they sought to delay such notice.[27]

By forcing law enforcement agencies to contact the webmail provider in order to determine a suspect's IP address, the webmail provider can also act as a choke point, carefully evaluating each request for information and rejecting those that do not meet the appropriate standard or that come from a

---

25. Chester Wisniewski, *Facebook Notifications Leak IP Addresses*, DIGITALTHREAT.NET (May 8, 2010), http://www.digitalthreat.net/2010/05/facebook-notifications-leak-ip-addresses.

26. *See* Matt C., *Facebook Leaks IP Addresses*, BINARY INTELLIGENCE (May 7, 2010), http://www.binint.com/2010/05/facebook-leaks-ip-addresses.html.

27. 18 U.S.C. § 2705 (2006).

foreign government that the provider has no legal obligation to assist. For example, in the event that a request comes from investigators in a foreign country, a service provider can often ignore the request and, thus, effectively protect the privacy of their customers. In such situations, this minor speed bump becomes a highly effective privacy tool.

Consider a scenario in which a pro-democracy activist in Vietnam, Zimbabwe, or some other oppressive regime is using their U.S.-based webmail provider to send out documents. Should state security officials obtain one of the email messages sent by the activist, the choice of webmail provider will significantly impact their ability to determine her identity. If the activist uses Google's Gmail service, the only way for the authorities to learn her IP address will be to contact Google and ask for the information—something the company is highly unlikely to provide. If, on the other hand, the activist uses Microsoft Hotmail or Yahoo! Mail, the state security officials will be able to locate her IP address in the header of the received email and to go directly to her domestic ISP in order to identify the activist. Even if Yahoo! or Microsoft have an official policy of not cooperating with the authorities in Zimbabwe or Myanmar, it will do the user no good.

By automatically including the user's IP address in the headers of outbound email messages, Microsoft, Yahoo, and, until recently, Facebook have robbed themselves of the ability to protect their users from unreasonable or illegal law enforcement investigations.

B. COMMUNITY OF INTEREST DATABASES

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 a security tool to see if new customers called the same numbers as previously cut-off fraudsters—something the original researchers referred to as "guilt by association."[28] However, the government soon took an interest in the ability to

28. *See* Corinna Cortes et al., *Communities of Interest*, 2189 PROCEEDINGS OF THE 4TH INT'L CONF. ON ADVANCES IN INTELLIGENT DATA ANALYSIS 105, 110–11 (2001) (describing the tendency of 'fraudsters' to have closer links to other 'fraudsters' than a random account would have).

sift through the telecom giant's vast databases.

In 2007, it was revealed that Federal Bureau of Investigation (FBI) had been seeking "community of interest" or "calling circle" records from several telecommunications providers via National Security Letters, grand jury subpoenas, exigent letters, and email requests. [29] 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.[30]

A subsequent investigation by the Inspector General of the Department of Justice (DOJ) found that these powers had been widely abused by the FBI. [31] 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."[32]

AT&T was not the only telecommunications carrier to have embedded employees within the FBI unit that abused its powers—Verizon, too, had employees on site. As such, Verizon received subpoenas and NSLs containing requests to "identify a 'calling circle' for the foregoing telephone numbers based on a two-generation community of interest [and] provide subscriber information."[33] However, because the company did not maintain a community of interest database, it was able to simply ignore that component of the requests it received.[34]

---

29. *See* Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets*, N.Y. TIMES, Sept. 9, 2007, *available at* http://www.nytimes.com/2007/09/09/washington/09fbi.html#.

30. *Id*.

31. *See* OFF. OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS (2010).

32. *Id*.

33. Milch*, supra* note 1, at 13 ("Verizon has also received subpoenas and NSLs containing 'boilerplate' language directing us, for example, to 'Identify a 'calling circle' for the foregoing telephone numbers based on a two-generation community of interest; provide subscriber information.' Because Verizon does not maintain such 'calling circle' records, we have not provided this information in response to these requests; we have not analyzed the legal justification for any such requests, been offered indemnification for any such requests, or sought our customers' consent to respond to such any such requests.").

34. *Id*.

The original researchers who created AT&T's community of interest system likely did not plan for their tool to be used to further government surveillance. However, once AT&T had the system in place, the government could compel its use. Verizon effectively protected its customers' privacy against fishing expeditions and other large-scale requests for information by not deploying a similar system.

C. PROACTIVE SEARCHES FOR CHILD PORNOGRAPHY

Federal law requires that ISPs immediately notify the appropriate authorities when they detect or otherwise learn about the presence of child pornography on their servers.[35] 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 flagged by their users or other third parties.[36]

The law does not, however, require that ISPs seek out such materials by automatically analyzing their customers' communications. Nevertheless, several ISPs have opted to do so.

In 2002, AOL developed and began using a proprietary Image Detection and Filtering Program (IDFP), which calculates a cryptographic hash (or fingerprint) of each file attached to email messages sent or received by its subscribers and then compares these hashes to a database of hashes for images that AOL has previously identified as images depicting child pornography. In the event that AOL's IDFP system detects the attachment of known child pornography, the company notifies the National Center for Missing and Exploited Children (NCMEC) as required by law.[37]

According to court filings by the company, "AOL developed and began using the IDFP in 2002 in order to protect its rights and property against lawbreakers, prevent the network from being used to carry or store contraband (i.e., illegal child pornography), and fulfill its legal obligation to report the

35. 18 U.S.C. § 2258A (2006).

36. *See, e.g.*, Brad Stone, *Policing the Web's Lurid Precincts: An Emotional Toll on Guardians Against Depravity*, N.Y. TIMES, July 19, 2010, at B1 (describing the efforts of large tech companies such as Microsoft, Yahoo!, MySpace, and YouTube to review content flagged as inappropriate).

37. United States v. Richardson, 607 F.3d 357, 363 (4th Cir. 2010).

transmission . . . of child pornography on its systems."[38]

Child pornography is an issue that plagues the debate over online privacy. No one wants 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 the privacy of normal users can and should be sacrificed in order to assist in the government's attempts to detect and prosecute such crimes. While many ISPs and legal experts have reservations about the tactics used by government investigators, prosecutors, and the quasi-governmental NCMEC, few will go on record to air such complaints.[39]

AOL's decision to proactively scan its customers' email attachments for child pornography has a major impact on their privacy, and, more importantly, the impact of this system extends far beyond the company's desire to assist in the discovery of such illegal content. The reason for this is that once a technical infrastructure 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.[40] Thus, AOL's automatic email attachment analysis system could also be used to determine if its customers are transmitting bomb making instructions, copyrighted images, songs and books, seditious newsletters, or religious texts. The government can simply provide the company with a list of additional hashes to add to the company's database and then wait for AOL to detect the transmission of such files.[41]

AOL's intentions may have been pure when the company dedicated engineering time to developing its email attachment scanning system, and it is quite possible that the vast majority of its customers might even approve of such a service and the associated intrusion into their communications privacy if they

38. *Id*.

39. Christopher Soghoian, *Editorial: It's Time for a Child Porn Czar*, SURVEILLANCE STATE (Dec. 9, 2008, 7:00 AM), http://news.cnet.com/8301-13739_3-10118923-46.html (recounting the reluctance of experts in the field of Internet law and policy to go on record to voice their criticism of the NCMEC).

40. *See* Miles Benson, *In the Name of Homeland Security, Telecom Firms are Deluged with Subpoenas*, GLOBAL RESEARCH (Dec. 30, 2005), http://www.globalresearch.ca/index.php?context=va&aid=1677 (quoting telecom lawyer Al Gidari describing this phenomenon as, "if you build it, they will come").

41. There is no evidence to suggest that AOL has ever searched for anything but child pornography using the database of hashes it has created itself.

knew it is occurring. However, the service may eventually be used for far more dubious law enforcement purposes, some of which AOL's customers are unlikely to consider reasonable.

While AOL was the first ISP to embrace this practice, it is not the only company to do so. In June 2010, several large social networks, including Facebook and MySpace, announced that they would begin scanning their customers' uploaded images against a database of child pornography hash signatures provided by the New York Attorney General.[42]

D. ENCRYPTION

Encryption technologies have been readily available to consumers for more than a decade, are now included in all modern operating systems and web browsers, and, as such, are widely used by many companies. Many companies use encryption technologies to protect the transmission of sensitive data (such as credit card numbers) between a customer's computer and a company's server. However, some firms are increasingly also encrypting users' data in storage so that no one other than the end user (including the service provider) can access the data.

Telecommunication carriers and technology firms in the United States are legally free to add encryption capabilities to their products.[43] However, a firm's legal obligations to provide the government with access to users' data differ based on the provider's ability to access the encryption key used to encrypt the data. If a company does not have access to the encryption key or to other "information necessary to decrypt the

42. *Attorney General Cuomo Announces Additional Social Networking Sites Join His Initiative To Eliminate Sharing Of Thousands Of Images Of Child Pornography*, OFF. N.Y. ATT'Y GEN. (June 29, 2010), http://www.ag.ny.gov/media_center/2010/june/june29a_10.html.

43. H.R. REP. NO. 103-827, pt. 1, at 25 (1994) ("Finally, 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. This obligation is consistent with the obligation to furnish all necessary assistance under 18 U.S.C. Section 2518(4). Nothing in this paragraph 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 the bill is intended to limit or otherwise prevent the use of any type of encryption within the United States. Nor does the Committee intend this bill to be in any way a precursor to any kind of ban or limitation on encryption technology. To the contrary, section 2602 protects the right to use encryption.").

communication," it has no legal obligation to decrypt its users' data or to otherwise ensure the government's ability to decrypt any subscriber encrypted communication.[44] However, if the company does have a copy of (or access to) the decryption key, it can be compelled to decrypt the user's data.[45]

1. Transport Encryption

The use of encryption to protect users' private information in transit brings multiple privacy benefits: it limits the ability of cyber-criminals and other nefarious persons to intercept data and even hijack users' accounts, it prevents the analysis of users' communications by ISPs using Deep Packet Inspection hardware in order to deliver behaviorally targeted advertising, and it effectively thwarts network-based surveillance by government agencies, forcing them to go directly to the company storing the data, rather than being able to passively intercept it in transit with the assistance of an ISP.[46]

While the banking and finance industries long ago adopted SSL transport encryption (enabling users to securely e-bank at home), the vast majority of cloud computing services are today, by default, insecure. This is because most consumer-aimed cloud services do not use common encryption technologies to protect user data in transit.[47] However, a few cloud computing firms, such as Google, have opted to encrypt user data in

44. *Id*. at 39.

45. *See, e.g.,* 47 U.S.C. § 1002(b)(3) (2006) ("A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.").

46. *See generally* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417 (describing the necessary balance between user privacy and ISP need).

47. *See* Predrag Klasnja et al., *"When I am on Wi-Fi, I am Fearless:" Privacy Concerns & Practices in Everyday Wi-Fi Use*, 2009 PROCEEDINGS OF THE 27TH INT'L CONF. ON HUMAN FACTORS IN COMPUTING SYS. 1993, *available at* http://www.seattle.intel-research.net/pubs/p1993-klasnja.pdf ("A majority of the large Web-based email services, for example, encrypt the login process, but not the contents of email messages. Anyone along the path between the user and the service's data center could intercept this information, opening users to privacy and security risks."); Letter from Jacob Appelbaum et al. to Eric Schmidt, CEO, Google, Inc. (June 16, 2009), *available at* http://www.cloudprivacy.net/letter ("Google is not the only Web 2.0 firm which leaves its customers vulnerable to data theft and account hijacking. Users of Microsoft Hotmail, Yahoo Mail, Facebook and MySpace are also vulnerable to these attacks.").

transit, in some cases by default.

When Google launched its Gmail email service in 2004, it offered SSL transport encryption as an option, albeit one not enabled by default. Likewise, when the company later rolled out its Docs, Spreadsheets, and Calendar apps, they, too, could be accessed via SSL but, again, not by default. However, in June 2009, thirty-eight industry and academic experts from the fields of computer security, privacy, and law (led by this author) wrote an open letter to Google's CEO to chastise the company for its lack of default transport encryption.[48] Seven months later, the company enabled HTTPS encryption by default for its Gmail service, and, approximately six months after that, also enabled encryption for its Docs, Spreadsheets, and Calendar services, too.[49] Similarly, in May 2010, the company began to offer SSL encrypted search, making it the first major search engine to do so.[50]

Following Google's lead, or perhaps feeling increased pressure from consumer protection regulators,[51] Microsoft, in November 2010, started to offer SSL protection for its popular Hotmail service, although not enabled by default.[52]

48. *See* Appelbaum, *supra* note 48; *see also* Ryan Singel, *Encrypt the Cloud, Security Luminaries Tell Google – Update*, WIRED (June 16, 2009), http://www.wired.com/threatlevel/2009/06/google_ssl (reporting on the letter from security researchers to Google and the company's response).

49. *See* Sam Schillace, *Default HTTPS Access for Gmail*, THE OFFICIAL GMAIL BLOG (Jan. 12, 2010, 9:14 PM), http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html (describing the process behind the decision to enable HTTPS encryption by default).

50. *See* Evan Roseman, *Search More Securely with Encrypted Google Web Search*, THE OFFICIAL GMAIL BLOG (June 25, 2010, 12:30 PM), http://googleblog.blogspot.com/2010/05/search-more-securely-with-encrypted.html (announcing the option for encrypted searches on Google).

51. Pamela Jones Harbour, Comm'r, Fed. Trade Comm'n, Remarks Before Third Fed. Trade Comm'n Exploring Privacy Roundtable in Washington, D.C. (March 17, 2010) *available at* http://www.ftc.gov/speeches/harbour/100317privacyroundtable.pdf ("My bottom line is simple: security needs to be a default in the cloud. Today, I challenge all of the companies that are not yet using SSL by default. That includes all email providers, social networking sites, and any website that transmits consumer data. Step up and protect consumers. Don't do it just some of the time. Make your websites secure by default.").

52. *See* Dick Craddock, *Hotmail Security Improves with Full-Session HTTPS Encryption*, INSIDE WINDOWS LIVE BLOG (Nov. 09, 2010), http://windowsteamblog.com/windows_live/b/windowslive/archive/2010/11/09/hotmail-security-improves-with-full-session-https-encryption.aspx.

The thirty-eight experts who pushed Google to enable SSL by default, and the FTC Commissioner who later pushed for other companies to do the same, all called for the use of encryption to address a single threat: hackers and other criminals who can otherwise easily snoop on consumers as they connect to cloud based services from public wireless Internet networks. Not mentioned was the equally real threat of surveillance by governments around the world, made possible with the assistance of major telecommunication carriers who have given intelligence agencies access to their backbone networks.[53]

Whatever the motivation for the switch to SSL, Google's decision had a very real impact on the ability of many foreign governments to spy on their citizens' communications (at least in those countries in which Google does not respond to subpoenas or other formal requests). For example, just one month after Google enabled SSL by default for Gmail, the Iranian government blocked all domestic access to Google's email service.[54] According to media reports, communications experts believe that the Iranian authorities' decision to block Gmail was in response Google's adoption of encryption by default.[55] Yahoo! and Hotmail, neither of which offers encryption by default, were not blocked by the Iranians.

2. Storage Encryption

Cloud-based services do not, by their very nature, have to store their users' data in the clear and, consequently, put the privacy of their users at risk. Consider as an example the Firefox Sync feature in the Firefox web browser.[56] This feature enables users to keep their bookmarks, browsing history, saved passwords, and cookie synchronized across multiple computers. The feature includes support for the Firefox mobile browser, allowing users to bookmark a web page at home and then view

53. *See generally* Siobhan Gorman, *NSA's Domestic Spying Grows As Agency Sweeps Up Data: Terror Fight Blurs Line Over Domain; Tracking Email*, WALL ST. J., Mar. 10, 2008, at A1 (reporting on the large amount of electronic records spy agencies now monitor).

54. *See* Nazila Fathi, *Iran Disrupts Internet Communications,* N.Y. TIMES, Feb. 11, 2010, at A6.

55. *Id.*

56. *See Sync*, MOZILLA, https://www.mozilla.com/en-US/firefox/sync/ (last visited Oct. 14, 2010).

it later in the day from their phone or other portable device.[57]

Like all cloud services, The Mozilla Corporation (which makes Firefox) is able to provide this instant, worldwide access by allowing users to store their own data on the company's servers. However, Mozilla baked privacy into the product at the design stages, stating that a key principle of the project is that "users own their data, and have complete control over its use. Users need to explicitly enable third parties to access their data."[58] As a result, the data that Sync users store on Mozilla's servers is encrypted with a key created by that user and which is not shared with anyone else. Mozilla provides the cloud-based storage, but is unable to peek at its users' stored passwords and browsing history.[59] In the event that law enforcement or intelligence agencies seek to compel Mozilla to share its users' data, the company can confidently hand over the encrypted files with the knowledge that the data is complete gibberish to everyone but its owner.

Mozilla is not the only organization to use encryption to securely store users' data in the cloud. Over the past several years, numerous companies have started to offer cloud-based backup solutions that enable users to automatically store their personal documents and other important files online.[60] However, of all these services, SpiderOak has opted to build strong encryption into their product by default.[61] The company describes itself as a "'zero knowledge backup provider," arguing, "[W]e 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." Other than its strong encryption feature, the service is remarkably similar to the numerous other products in the online backup market.[62]

57. *Id*.

58. *Services/Sync/FxSync/Archived/OAuth*, MOZILLA WIKI, https://wiki.mozilla.org/Labs/Weave/OAuth (last modified July 12, 2010).

59. *Id*.

60. These include Dropbox, Box.net, Sugarsync, Elephantdrive, and Microsoft Live Mesh.

61. *Free Windows, Mac and Linux Online Backup, Online Sync, Share & Storage from SpiderOak.com*, SPIDEROAK.COM, https://www.spideroak.com (last visited Sept. 30, 2010).

62. *Engineering Matters*, SPIDEROAK.COM, https://spideroak.com/engineering_matters#true_privacy (last visited Sept. 30, 2010); *Frequently Asked Questions*, SPIDEROAK.COM,

Currently, the major Internet giants such as Google, Microsoft, and Facebook have yet to add any form of secure storage encryption to their products. One reason for this may be that these products are largely supported by targeted advertising, which often relies upon the ability to look through the plain text of users' communications and other private data. Unfortunately for these firms, it is exceedingly difficult to monetize a data set that one cannot look at.[63] If these firms do eventually decide to offer encrypted cloud based storage, it is likely first to be to the enterprise customers who are charged a fee to use the firms' services.

E. DATA RETENTION POLICIES

The decision to delete data is often one of the most effective ways in which a company can preserve the privacy of its customers. There are both direct and indirect costs for keeping data. The costs of the storage technology (e.g., hard disks, backup tapes) shrink every year, making it increasingly cheap to retain data. However, the increasing costs of personal information handling rules, data breaches, and lawsuits do appear to be providing some companies with an economic incentive to delete data once they no longer need it.[64]

As such, most technology providers and communications

https://spideroak.com/faq/does_spideroak_use_encryption_when_storing_and_transferring_data (last visited Sept. 30, 2010).

63. Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH L. 359, 397 (2010) ("It is exceedingly difficult to monetize a data set that you cannot look at. Google's popular Gmail service scans the text of individual emails, and algorithmically displays relevant advertisements next to the email. When a user 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 is unable to scan the contents and display related advertising. Sure, the company can display generic advertisements unrelated to the user's communications contents, but these will be far less profitable.").

64. *See* Ellen Messmer, *Data Breach Costs Top $200 per Customer Record*, NETWORKWORLD (Jan. 25, 2010), http://www.networkworld.com/news/2010/012510-data-breach-costs.html ("The cost of a data breach increased last year to $204 per compromised customer record, according to the Ponemon Institute's annual study. The average total cost of a data breach rose from $6.65 million in 2008 to $6.75 million in 2009."); Holly Towle & Scott L. David, *Is Data Like Toxic Waste?*, K&L GATES, http://www.engr.washington.edu/epp/infosec/presentations/Sep%2016%20data%20as%20toxic%20asset%20presentation%20as%20sent%20V2.ppt (last visited Sept. 30, 2010) ("Data protection laws have turned Personal Information ("PI") into the intangible equivalent of toxic waste.").

carriers now have established data retention policies that govern the length of time before which they will delete customer records, communications, logs, and other data. Unfortunately, outside of the search engine market, where pressure from European regulators has lead to companies publicly touting their policies, few other firms will publicly reveal their own data retention rules.[65]

The widespread lack of public information about data retention policies poses a significant problem for consumers wishing to evaluate potential service providers on their respective privacy merits. Furthermore, differences among providers operating in the same market do vary considerably, which means that the decision to pick a particular service provider can have a significant impact on a user's privacy.

A great example of this is seen in the wireless telephone market. Sprint Nextel assigns each Internet-connected wireless handset a static IP address and logs the allocation of these addresses for a twenty-four month period.[66] The company also logs the URL of each webpage viewed by its customers, whose handsets route requests through the company's WAP Media Access Gateway proxy server.[67] In contrast, both T-Mobile and

65. *Compare* Peter Fleischer, Jane Horvath & Alma Whitten, *Another Step to Protect User Privacy*, OFFICIAL GOOGLE BLOG, (Sept. 8, 2008, 7:06 PM), http://googleblog.blogspot.com/2008/09/another-step-to-protect-user-privacy.html (explaining how Google's data retention policy is affected by EU, and other, regulators), *with Sprint Nextel International Data Privacy Policy*, SPRINT, http://shop.sprint.com/en/solutions/sprint_worldwide/international_data_privacy_popup.shtml (last visited Nov. 13, 2010) ("Sprint Nextel retains all of the information it collects under this Privacy Policy in compliance with applicable law and as long as there is a business need for it. In addition, we have a record retention policy that generally implements the broad range of regulatory requirements imposed on service providers for recordkeeping.").

66. Paul Taylor, Elec. Surveillance Manager, Sprint Nextel, Address at the ISS World Conference, Washington DC, (Oct. 13, 2009) (audio available at http://www.eff.org/files/soghoian-surveillance-dump.zip) ("Nextel's system, they statically assign IP addresses to all handsets . . . . We do have logs, we can go back to see the IP address . . . . On the Sprint 3G network, we have IP data records back 24 months, and we have, depending on the device, we can actually tell you what URL they went to . . . . If [the handset uses] the [WAP] Media Access Gateway, we have the URL history for 24 months . . . . We don't store it because law enforcement asks us to store it, we store it because when we launched 3G in 2001 or so, we thought we were going to bill by the megabyte . . . but ultimately, that's why we store the data . . . . It's because marketing wants to rifle through the data.").

67. *Id.*

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.[68] Consequently, the companies are unable to reveal after-the-fact which particular customer was responsible for traffic originating from their network.[69]

As a result of these policies, a Sprint Nextel customer can later be tracked down based on an anonymous comment left on a blog or a peer-to-peer (P2P) file downloaded over the company's cellular network, while customers of T-Mobile and Cricket can freely engage in a variety of online activities without any risk of later discovery.

While most companies are not willing to disclose their data retention periods to their customers or to queries from members of the privacy community, they seem quite willing to voluntarily provide this information to the law enforcement community. Most Internet and telecommunications providers have created law enforcement handbooks, which, in addition to providing "boilerplate" sample subpoenas and search warrant applications, also detail the kinds of data that each firm retains and for how long. Over the last year, many of these law enforcement handbooks have surfaced on the Internet, much to the displeasure of their creators.

These law enforcement handbooks enable, for the first time, some degree of transparency in this area. I have created Table 1 based on the handbooks that have been leaked thus far. Clearly, many companies are missing from the table—but

68. Janet A. Schwabe, Subpoena Compliance Manager, Cricket Communications, Address at the ISS World Conference, Washington D.C. (Oct. 13, 2009) (audio available at http://www.eff.org/files/soghoian-surveillance-dump.zip at approximately 105:00).

69. *See, e.g.*, Gavin Pinchback, Director, Law Enforcement Relations, T-Mobile USA, Address at the ISS World Conference, Washington D.C. (Oct. 13, 2009) (audio available at http://www.eff.org/files/soghoian-surveillance-dump.zip at approximately 108.09) ("[T-mobile is] in the same boat that Cricket is, in terms of determining the IP address—determining the subscriber attached to that IP address."); Schwabe, *supra* note 68 ("One of the challenges for Cricket, and a challenge for the law enforcement community, is that we now have broadband and internet access from the handset. And in both instances, the signal goes to our switch, and then is relayed to Level 3 Communications, which then is the conduit to the Internet. From the outside, from the point of capture of the IP address, it is the generic or regional IP address that is picked up. There is no way to come back through our firewall to see which subscriber had a per-session identification on that, and that is something that even if you go to Level 3, they're not going to have any information either.").

compared to what was known one year ago, this is a great step in the right direction (even if it was not accomplished with the assistance or consent of the firms whose policies have been revealed).

Table 1. Data Retention Policies

Company	IP Address Login Data Retained	Account Registration Information Retained
Microsoft	60 days[70]	Life of account.
Yahoo	6 months[71]	Life of account + 90 days after deletion.
AOL	90 days[72]	*Unknown*
MySpace	1 year[73]	Life of account + 90 days after deletion.
Facebook	Generally 90 days[74]	Unknown
Time Warner Cable	6 months[75]	Unknown

70. Global Criminal Compliance Handbook 6, Microsoft Online Services (Mar. 2008), *available at* http://cryptome.org//isp-spy/microsoft-spy.zip [hereinafter Microsoft].

71. Compliance Guide for Law Enforcement 4–5, Yahoo!, *available at* http://cryptome.org/isp-spy/yahoo-spy.pdf (last visited Oct. 14, 2010) [hereinafter Yahoo!]. The company has since reduced its data retention period for most logs to six months. Press Release, Yahoo!, Inc., Yahoo! Sets New Industry Privacy Standard with Data Retention Policy (Dec. 17, 2008), http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=354703.

72. Public Safety & Criminal Investigations 18, AOL (Sep. 2008), *available at* http://cryptome.org/isp-spy/aol-spy.pdf.

73. Law Enforcement Investigators Guide 7, MySpace, *available at* http://cryptome.org/isp-spy/myspace-spy.pdf (November 1, 2007) (on file with Minnesota Journal of Law, Science & Technology) [hereinafter MySpace 2007]. For a previous version stating MySpace retains IP data for 90 days, see Law Enforcement Investigators Guide 7–8, MySpace, *available at* http://cryptome.org/isp-spy/myspace-spy.pdf (last updated June 23, 2006) [hereinafter MySpace 2006].

74. Subpoena/Search Warrant Guidelines 5, Facebook (Feb. 2008), *available at* http://cryptome.org/isp-spy/facebook-spy.pdf [hereinafter Facebook]. See *Confidential Facebook Law Enforcement Subpoena Guides 2007–2010*, PUB. INTELLIGENCE (OCT. 6,2010), http://publicintelligence.net/confidential-facebook-law-enforcement-subpoena-guides-2007-2010 for copies of Facebook's Law Enforcement Subpoena Guides for the years 2007–2010.

75. Nate Anderson, *Time Warner Cable Tries to Put Brakes on Massive Piracy Case*, ARS TECHNICA, http://arstechnica.com/tech-policy/news/2010/05/time-warner-cable-tries-to-put-brakes-on-massive-piracy-case.ars ("TWC has a six-month retention period for its IP lookup logs, and by the time TWC could turn to law enforcement requests, many of these requests

1. Data Retention Creep

One significant problem stemming from the widespread industry practice of firms not disclosing their data retention policies is that consumers are completely unaware of changes to those policies. Worse is that, other than in the case of the search engines (who are under intense regulatory pressure to keep less and less data), data retention policy changes usually occur in only one direction: towards greater retention.

For example, over the last year or two, multiple wireless carriers have 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, a significant increase over the thirty days or fewer that the data was retained two years ago.[76] Similarly, between 2007 and 2008, MySpace and Facebook both increased their data retention periods for user login IP session data. In 2006, MySpace logged IP addresses associated with account logins for ninety days. In 2007, the company expanded its logging of this data to one year.[77] Facebook logged IP addresses for thirty days in 2007, but, by 2008, the company had opted to keep the logs for ninety days.[78]

These social networking 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 period, let alone the new one). Instead, the only mentions of the changes were made in updated handbooks provided to law enforcement agencies.

In most cases, the move to increase data retention seems to have been a voluntary decision on the part of the carriers. In other 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)."[79] Needless to say,

---

could not be answered.") (last updated May 2010).

76. Declan McCullagh, *Feds Push for Tracking Cell Phones*, CNET NEWS (Feb. 11, 2010), http://news.cnet.com/8301-13578_3-10451518-38.html.

77. *Compare* MySpace 2007, *supra* note 73, at 7, *with* MySpace 2006, *supra* note 73, at 7–8.

78. Facebook, *supra* note 74, at 5.

79. *Communication Exploitation*, WIRED,

neither Verizon nor AT&T, two of the firms that received millions of dollars to provide the FBI access to their customers' data, opted to inform their customers that the firms were entering into these relationships to monetize their data and increase the ease with which it could be disclosed to FBI agents.

2. The Impact of Zero Data Retention Policies—Or Unintended Consequences of the Copyright Lobby

Although none of the major U.S.-based Internet application providers and telecommunications carriers have adopted zero data retention policies, several large companies in other counties have done just that, as have smaller firms in the United States. These policies have had a direct impact on the ability of law enforcement authorities to compel the disclosure of data. Simply put, when no data is retained, there is nothing to deliver when a subpoena later arrives.

In April 2009, Sweden enacted a controversial law that grants copyright holders the authority to request the personal details of alleged infringers from ISPs. The response from consumers was swift—Swedish Internet traffic dropped by over thirty percent starting the day that the new law came into effect.[80] This clear demonstration of consumers' privacy fears then led to rapid competition in the market for privacy-preserving services.

Within weeks, three of Sweden's ISPs announced new zero data retention policies for the IP addresses provided to broadband customers. Explaining the motivation for change in policy, the CEO of one of the country's largest ISPs said, "[I]t's a strong wish from our customers, so we decided not to store information on customers' IP numbers."[81]

The adoption of these zero data retention policies has

---

http://www.wired.com/images_blogs/threatlevel/files/communicationsexploitationoffice08budget.pdf (last visited Oct. 14, 2010).

80. *Piracy Law Cuts Internet Traffic*, BBC NEWS (Apr. 2, 2009), http://news.bbc.co.uk/2/hi/technology/7978853.stm ("The new law, which is based on the European Union's Intellectual Property Rights Enforcement Directive (IPRED), allows copyright holders to obtain a court order forcing ISPs to provide the IP addresses identifying which computers have been sharing copyrighted material. . . . [T]raffic fell from an average of 120Gbps to 80Gbps on the day the new law came into effect.").

81. Mats Lewan, *Swedish ISPs Vow to Erase users' Traffic Data*, CNET NEWS (Apr. 28, 2009), http://news.cnet.com/8301-1023_3-10229618-93.html.

generated unintended consequences beyond the area of copyright enforcement. In May 2010, the head of the Swedish Police's National IT crime unit told one newspaper that, due to a lack of customer logging data at ISPs, it has become much harder for the police to trace and identify criminal suspects.[82]

Outside of Sweden, the threat of copyright lawsuits has also almost singlehandedly created a growth industry in commercial anonymous Virtual Private Network (VPN) providers that openly advertise zero log retention polices and through which users of peer-to-peer software can download content without fear of being identified.[83] Of course, these services' zero log retention policies thwart investigations by law enforcement agencies, in addition to just Recording Industry Association of America (RIAA) lawyers.

III. STRICT INTERPRETATIONS OF THE LAW CAN ALSO RESTRICT GOVERNMENT ACCESS TO DATA

The Electronic Communications Privacy Act (ECPA)[84] details the instances in which telecommunications carriers and ISPs can and cannot disclose their customers' communications. With regard to government access, the law is quite specific in some areas, and, as such, when a company receives a valid subpoena, 2703(d) order, or search warrant, there is not much that the company can do other than disclose the data required of it. However, there are quite a few grey areas where several companies have adopted strict, pro-privacy interpretations of the law. This section outlines these grey areas, several of which have never before been publicly discussed.

---

82. *See* Enigmax, *Police Say Anti-Piracy Law Makes Catching Criminals Harder*, TORRENTFREAK (May 17, 2010), http://torrentfreak.com/police-say-anti-piracy-law-makes-catching-criminals-harder-100517.

83. *See, e.g.*, *FAQ & Support*, YOURPRIVATEVPN, http://www.yourprivatevpn.com/?q=en/faq_en (last visited Oct. 14, 2010) ("The servers are configured in such a way that they do not store IP addresses. . . . Our goal is to make our customers feel safe again. Therefore data, which we might be forced to hand over to authorities, is not being stored."); *Frequently Asked Questions*, PERFECT PRIVACY, http://www.perfect-privacy.com/faq.html (last visited Oct. 14, 2010) ("For the privacy and anonymity of our members we have disabled logging."); *Torrent Freedom,* TORRENT FREEDOM, http://torrentfreedom.com (last visited Oct. 14, 2010) ("We'll make your traffic completely transparent. Anonymity is our business."); *Welcome to FlashVPN*, FLASHVPN.COM, http://www.flashvpn.com (last visited Oct. 14, 2010) ("No provider logs").

84. Pub. L. No. 99-508 § 1 (codified as amended in scattered sections of 18 U.S.C.).

A. OPENED EMAILS AND *THEOFEL*

18 USC 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."[85]

There has been considerable debate about the definition of the term "electronic storage," as the DOJ has taken the position that once an email message has been opened, it is no longer in electronic storage and, thus, can be divulged pursuant to a subpoena or 2703(d) order.[86]

The government's narrow interpretation of "electronic storage" was rejected by the Ninth Circuit in *Theofel v. Farey-Jones,*[87] in which the court held that email messages continue to be in "electronic storage" regardless of whether they have been previously accessed.[88] As such, prosecutors within the Ninth Circuit are bound by *Theofel*. However, the DOJ has taken the position that law enforcement elsewhere may continue to apply the traditional narrow interpretation of "electronic storage," and obtain opened emails with a mere subpoena even when the data sought is held on servers located within the Ninth Circuit.[89]

Many large ISPs 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.[90] Others have simply argued that they believe that *Theofel* is the correct interpretation of the law, and opened emails should not lose their protection under the law, regardless the location of the ISP or the requesting government

85. 18 U.S.C. 2703(a) (2006).

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

87. *Id*.

88. *Id*.; *see generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

89. DEPT. OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE MANUAL (Sep. 2009), *available at* http://www.justice.gov/criminal/cybercrime/ssmanual/03ssma.html.

90. U.S. v. Weaver, 636 F. Supp. 2d 769 (C.D. Ill. 2009) ("Microsoft asserts that because its headquarters are located within the Ninth Circuit, it must comply with Ninth Circuit precedent.").

agency.[91] 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.[92]

When ISPs receive a subpoena or 2703(d) order from outside the Ninth Circuit, they can either comply with the order or refuse and go to court. The companies that do refuse to comply with such orders rarely make this information public, and so it is exceeding difficult for consumers to easily evaluate an ISP's willingness to fight for this issue.

B. DELIVERING TO/FROM HEADERS IN RESPONSE TO SUBPOENAS FOR EMAIL MESSAGES

ISPs have significant flexibility in pushing back against government requests when the law is vague. One such example of this relates to the delivery or scrubbing of to/from headers in email messages over 180 days old that are provided to the government in response to a subpoena.

Section 2703(a) specifies that the government can use either a subpoena or a 2703(d) order to obtain the contents of email communications that are older than 180 days.[93] Non-content information,[94] however, can only be obtained pursuant to either a search warrant or a 2703(d) order.[95] Email headers

91. Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not A Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569, 580–581 (2007) (Despite continuing uncertainty as to the correctness of the *Theofel* reading of the backup storage provision, the decision in *Theofel* is followed by most major ISPs, who now require search warrants before producing any e-mail or private message content less than 180 days old."); *The ECPA, ISPs & Obtaining E-mail: A Primer for Local Prosecutors*, BUREAU OF JUSTICE ASSISTANCE (July 2005), *available at* http://www.ndaa.org/pdf/ecpa_isps_obtaining_email_05.pdf ("State and local law enforcement should also be aware that several large ISPs such as AOL, Yahoo, and Hotmail are currently providing email content to law enforcement only pursuant to an ECPA warrant based on Theofel . . . regardless of the location of the requesting governmental entity, service of the process, or maintenance of the records.").

92. *See, e.g.,* Government's Motion to Compel Compliance with 2703(d) Order at 3, In Re Application of the United States of America for an Order Pursuant to 18 U.S.C. 2703(d), MISC NO 09Y080-CBS (D. Colo. Mar. 9, 2010), http://www.eff.org/files/filenode/inreusaorder18/MotiontoCompel.pdf.

93. 18 U.S.C. § 2703(a) (2006).

94. *See* 18 U.S.C. § 2703(c)(3) (2006).

95. 18 U.S.C. § 2703(c) specifies that "[a] governmental entity may require a provider of electronic communication service or remote computing service to

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*.[96]

As a result, Yahoo!, Google, and Microsoft have quietly established policies of scrubbing the "to" and "from" headers from email messages delivered to law enforcement agents in response to a subpoena.[97] In such instances, if government officials wish to compel the disclosure of the headers from these three companies, they must first obtain a § 2703(d) order or search warrant. By taking this position, these ISPs have been able to force some degree of judicial review over a process that would otherwise bypass the courts.

Multiple sources state that the DOJ does not favor the interpretation of ECPA adopted by these ISPs,[98] but it has not

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." 18 U.S.C. § 2703(c) (2006) (emphasis added). 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)." 18 U.S.C. § 2703(c)(2)(a)–(f) (2006).

96. United States v. Forrester, 512 F.3d 500, 503 (9th Cir. 2008) ("[E]-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers. When the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed.").

97. I have contacted representatives from most of the major ISPs, 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/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 the same strict 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 practices of Microsoft's competitors.

98. *E.g.*, Email from Richard Downing, Assistant Deputy Chief of the Computer Crime and Intellectual Property Section, Department of Justice, to Author (Jan. 28, 2010, 9:36 AM) (on file with author) (refusing to comment). I

gone to court to compel the delivery of these headers pursuant to a subpoena. It is unclear if the DOJ is worried about a negative ruling or if it wishes to avoid any public discussion about ISPs' ability to adopt such policies, fearing that other ISPs might do so if they knew they could.

It also remains unclear why Google, Yahoo! and Microsoft will not publicly confirm their interpretation of ECPA. As for the companies that still do not scrub the headers, there is likely a good reason why these companies refuse to admit it: the possibility of civil liability for improperly disclosing non-content communications information.[99]

As a result of this industry-wide trend of not commenting on the practice, it is practically impossible for consumers to evaluate their ISPs' positions on this obscure, yet important aspect of ECPA.

C. VOLUNTARY DISCLOSURES IN EMERGENCY SITUATIONS

While ECPA specifies the scenarios in which the government can compel an ISP to disclose its customers' communications, it also provides for voluntary disclosure in so-called exigent circumstances.[100]

18 U.S.C. § 2702(b)(8) and 18 U.S.C. § 2702(c)(4) similarly permit the disclosure of communications content and non-content:[101] "[T]o 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."[102]

This language has been repeatedly watered down over the past decade,[103] often due to requests from telecommunications

---

am still waiting for the results of a related FOIA request for information.

99. *See Quon v. Arch Wireless*, 529 F.3d 892, 900 (9th Cir. 2008), *cert denied sub nom*, Mobility Wireless, Inc. v. Quon, 130 S. Ct. 1011 (U.S., 2009) (on the issue of liability under the Stored Communications Act), and rev'd sub nom. City of Ontario v. Quon, 2010 U.S. LEXIS 4972 (U.S., June 17, 2010) (on the issue of validity of the search). The government may face additional administrative discipline measures under 18 U.S.C. § 2707(d). *See* 18 U.S.C. § 2707(d) (2006) (discussing administrative discipline under § 2707). *See also* 18 U.S.C. § 2712 (2006).

100. 18 U.S.C. § 2518(7)(a) (2006) (discussing the production of information in emergency situations).

101. 18 U.S.C. §§ 2702(b)(8), 2702(c)(4) (2006).

102. 18 U.S.C. § 2702(b)(8) (2006).

103. *See, e.g.,* Seth Rosenbloom, *Crying Wolf in the Digital Age: Voluntary Disclosure under the Stored Communications Act*, 39 COLUM. HUM. RTS. L.

carriers who do not want to be put in the position of evaluating the degree of the emergency.[104] There is little case law on the emergency provisions, although generally once a carrier receives a statement from the government certifying the emergency, it can disclose customers' communications without the risk of liability.[105]

Because the law does not require ISPs to tell their customers when their private communications or their non-content data associated with their private communications are voluntarily disclosed to the government, the likelihood that consumers ever learn of disclosures is extremely low. Furthermore, few companies will publicly discuss the extent to which they receive emergency requests, and federal reporting requirements for such requests are largely worthless.

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.[106] Of these 25,000 requests for emergency assistance, just 300 were from the federal government.[107] Verizon has not released any statistics detailing with how many of these 25,000 emergency requests it

---

REV 529, 559–561 (2008).

104. *See, e.g.*, DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS, 261 n.272 (Jan. 2010) (quoting H.R. Rep No. 107-497, at 12-13 (2002)), *available at* http://www.justice.gov/oig/special/s1001r.pdf ("The legislative history of a similar amendment to Section 2702(b)'s emergency voluntary disclosure provision for content information suggests that the belief standard was relaxed because communications service providers 'expressed concern to the Committee that the [reasonably believes] standard was too difficult for them to meet, and that as a result, providers may not disclose information relating to emergencies.'"); Milch, *supra* note 1; Luke O'Brien, *AT&T, Verizon: We Obeyed FBI "Emergency" Requests – 739 of Them,* WIRED (Mar. 21, 2007, 12:35 AM) http://www.wired.com/threatlevel/2007/03/att_verizon_we (quoting statement of Walt Sharp, AT&T Spokesperson, "'Failure to comply with an emergency request like this could endanger human life. We don't feel it's appropriate for a communications company to be second guessing a valid emergency request for assistance especially when it's followed up with the appropriate documentation.'").

105. *See, e.g.*, Jayne v. Sprint PCS, No. CIV S-07-2522 (E.D. Cal. Feb. 20, 2009) (rejecting ECPA lawsuit against Sprint PCS based on exigent circumstances letter claiming that the plaintiff was a kidnapper and that the records were needed to identify and locate the suspect and rescue his victim).

106. Milch, *supra* note 1, at 5.

107. *Id*.

refused to comply.

As the U.S. Internet Service Provider Association notes, "There is never an 'emergency' obligation on an ISP to disclose."[108] If a carrier 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.

Large ISPs and carriers often have vastly different policies when it comes to emergency requests, although none will publicly describe them. Occasionally, however, information about these practices does leak.

For example, in June 2009, an email message sent by a Florida police officer to others in the law enforcement community showed up on the wikileaks.org website.[109] That email described the officer's experiences interacting with several ISPs and telecommunication carriers during a recent child exploitation investigation.[110] 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 for logins that were more than 48 hours old. AT&T, however, 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 compelling disclosure.[111]

The area of voluntary disclosure is one of the most interesting, yet poorly understood areas in which companies have complete and total control over the information they provide to law enforcement. Some companies, such as AT&T,

---

108. U.S. Internet Serv. Provider Ass'n, *Electronic Evidence Compliance—A Guide for Internet Service Providers*, 18 BERKELEY TECH. L.J. 945, 962 (2003).

109. While it is difficult to guarantee that the email is not fictional, I have verified its authenticity with multiple well-informed sources. As such, I have reason to believe that the information contained within the email is valid. I have also attempted to get Yahoo! and AT&T to confirm the police officer's statements, but my contacts at the companies were not willing confirm, on or off the record. Email from Mike Duffy, Special Agent, Florida Department of Law Enforcement, to Internet Crimes Against Children Task Force Email List (June 26, 2009, 11:28 EST) (on file with author).

110. *Id.*

111. *Id.*

appear to have taken the position that, at least in some situations, they will not disclose information in emergencies. Other companies, such as Verizon, however, have argued in court that they have a First Amendment right to disclose their customers' private information to the government.

eBay's Director of Compliance and Law Enforcement Relations revealed the extent to which his company goes out of its way to voluntarily assist the government, stating in comments at a conference in 2003:

> We [eBay] try to make rules to make it difficult for people to commit fraud and easy for you [law enforcement agencies] to investigate . . . eBay has probably the most generous policy of any internet company when it comes to sharing information. We do not require a subpoena except [sic] for very limited circumstances. We require a subpoena when we need the financial information from the site, credit card info or sometimes IP information . . . if you are [a] law enforcement agency you can fax us on your letterhead to request information: who is that beyond the seller ID, who is beyond this user ID. *We give you their name, their address, their e-mail address and we can give you their sales history without a subpoena.*[112]

Since companies are 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. Thus, for example, it is unclear if AT&T has a blanket policy of refusing emergency requests, if it only refuses certain kinds of emergency requests, or if their decision, described above, was simply an isolated instance.

D. CHARGING THE GOVERNMENT FOR CONSUMERS' PRIVATE DATA

Many telecommunications companies and ISPs seek and typically receive payment from government agencies for the surveillance services they provide,[113] a practice that the law

112. *eBay to Law Enforcement – We're Here to Help*, LAWMEME (Feb. 17, 2003, 10:09 AM), http://lawmeme.research.yale.edu/modules.php?name=News&file=article&sid=925 (emphasis added).

113. If a provider sends the government agency an invoice for surveillance services, it does not mean the government agency will actually pay. "As part of our audit, we analyzed 990 telecommunication surveillance payments made by 5 field divisions and found that over half of these payments were not made on time. We also found that late payments have resulted in telecommunications carriers actually disconnecting phone lines established to deliver surveillance

often permits.[114] However, most firms opt to voluntarily waive the fees for certain types of investigations, and others have established policies of never charging 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.

There appears to be an industry-wide policy to not seek compensation regarding surveillance and data disclosures associated with child exploitation investigations. This is not required by law but seems to stem both from a wish by firms to be good corporate citizens, as well as a realistic awareness of the awesome rhetorical power that the child exploitation issue carries in the broader 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.

---

results to the FBI, resulting in lost evidence including an instance where delivery of intercept information required by a Foreign Intelligence Surveillance Act (FISA) order was halted due to untimely payment." OFFICE OF THE INSPECTOR GEN., THE FED. BUREAU OF INVESTIGATION'S MGT. OF CONFIDENTIAL CASE FUNDS AND TELECOMMUNICATION COSTS (Jan. 2008), *available at* http://www.justice.gov/oig/reports/FBI/a0803/index.htm.

114. Providers are prohibited by 18 U.S.C. § 2706(c) from recovering the cost of producing phone records. 18 U.S.C. § 2706(c) (2006). It is also unclear if providers who insist on a Rule 41 order to deliver location information can seek compensation (this is a position several providers, such as Loopt have taken). *See Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 29 (2010) (statement of Albert Gidari, Partner, Perkins Cole LLP). However, providers can seek compensation for most other 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." 18 U.S.C. § 2706(a) (2006). Further,"[a]ny provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance *shall be compensated therefore by the applicant for reasonable expenses* incurred in providing such facilities or assistance." 18 U.S.C. § 2518(4) (2006) (emphasis added). "[T]he Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to . . . immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition [and][t]he Government *shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance* in accordance with a directive issued pursuant to paragraph (1)." 50 U.S.C. §1881(a)(h)(1)-(2) (2006) (emphasis added).

In addition to the widespread practice of waiving charges for certain types of investigations, 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 it is a murder, terrorism, drug trafficking, or corporate fraud that is being investigated, these few technology firms have opted to provide their customers' data to the government for free. While there may be other companies that have established such policies, at least MySpace, Facebook, and Microsoft do not charge. MySpace's then-chief security officer confirmed that the company does not charge for the "thousands" of requests it receives from the government each year,[115] while well-informed sources confirmed similar policies at both Facebook and Microsoft.[116]

The impact of the decision to charge or not charge is significant, as telecommunications lawyer Al Gidari revealed recently in testimony before Congress:

> Service providers are prohibited by ECPA from recovering the cost of producing phone records, but service providers otherwise may recover costs reasonably necessary for the production of other subscriber information. *When records are 'free,' 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.*[117]

115. Interview with Hemanshu Nigam, Former Chief Sec. Officer, MySpace, in Washington D.C., (Feb. 4, 2010). I did not receive a reply to a follow-up email sent on the next day seeking information about the number of exigent requests the company receives, and the number of requests the company has refused to respond to.

116. Microsoft's law enforcement manual does not mention any policy of seeking compensation. *See* Microsoft, *supra* note 70. A well-informed source told me that the company does not charge for the information it provides in response to most requests, but reserves the right to charge the government when the information sought is particularly burdensome. Another well-informed source revealed that Facebook has a policy of not charging for government assistance, although its law enforcement manual does state the company reserves the right to do so. Facebook, *supra* note 74, at 2.

117. Hearing, *supra* note 100, at 29 (emphasis added).

E. PUBLISHING SURVEILLANCE PRICES

Although many service providers charge the government for access to their customers' data, few will publicly reveal the amount that they charge, if they charge anything at all.

Cox Communications is the only telecommunications provider that lists its surveillance prices on a publicly accessible page on its website.[118] However, the prices charged by several other companies have come to light over the past few years. Leaked law enforcement manuals for Yahoo!, Comcast, and Sprint detail the companies' surveillance prices,[119] while a letter sent by Verizon's General Counsel to members of Congress confirmed that the firm routinely requests compensation for the assistance it provides to law enforcement (without including the actual prices).[120] Likewise, Google's head of public policy revealed in comments at a public event in 2009 that the company requests compensation for the assistance it provides to the government.[121] Some firms have also attempted to use legal threats (both implied and overt) in order to stop the publication of their surveillance prices.

In September 2009, I filed Freedom of Information Act

118. *See Notice to Parties Serving Son Cox Communications*, COX COMMUNICATIONS, http://www.cox.com/Policy/leainformation/default.asp (last updated Oct. 1, 2009).

119. "Upon lawful request and for a thousand dollars, Comcast, one of the nation's leading telecommunications companies, will intercept its customers' communications under the Foreign Intelligence Surveillance Act. The cost for performing any FISA surveillance 'requiring deployment of an intercept device' is $1,000.00 for the 'initial start-up fee (including the first month of intercept service),' according to a newly disclosed Comcast Handbook for Law Enforcement (pdf). Thereafter, the surveillance fee goes down to '$750.00 per month for each subsequent month in which the original [FISA] order or any extensions of the original order are active.' Steven Aftergood, *Implementing Domestic Intelligence Surveillance*, SECRECY NEWS, (Oct. 15, 2007), http://www.fas.org/blog/secrecy/2007/10/implementing_domestic_intellig.html.

120. "Verizon has received compensation for reasonable costs incurred in complying with interception orders . . . for effecting pen/traps . . . for providing stored communications and customer records . . . for providing assistance in effecting electronic surveillance under [FISA] . . . and for effecting pen/traps under [FISA]." Milch *supra* note 1, at 10.

121. "At Computers, Freedom and Privacy last week, Google's DC policy guru Alan Davidson revealed that the company has between 1-20 employees working full time to respond to requests for private customer information from law enforcement. He also revealed that Google asks for financial compensation from the Government for the time required to satisfy these requests -- he noted that this practice is permitted by law." Christopher Soghoian, *A Shot Across the Bow*, SLIGHT PARANOIA (June 10, 2009, 12:35 PM), http://paranoia.dubfire.net/2009/06/shot-across-bow.html.

(FOIA) requests with several government agencies for copies of ISP surveillance price lists. Verizon's surveillance price list was among one of several documents in the possession of the U.S. Marshals Service that were responsive to my request. When given the opportunity to object to the disclosure of its price list, Verizon argued:

> [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).[122]

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

> [T]he [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.[123]

When a copy of Yahoo!'s law enforcement guide (which includes the price list) surfaced on the Internet website cryptome.org in December 2009, Yahoo!'s outside counsel attempted (and failed) to force the removal of the document from the whistleblower website via a Digital Millennium Copyright Act notice.[124] On the same day, Facebook sent me an email requesting that I remove a hyperlink from my personal Twitter account that linked to a copy of the company's law enforcement handbook that was hosted on the official website

122. Letter from Todd S. Schulman, Assistant General Counsel, Verizon, to Arleta D. Cunningham, U.S. Marshals Service (Sept. 14, 2009), *available at* http://files.cloudprivacy.net/verizon-price-list-letter.PDF.

123. Letter from Michael T. Gershberg, Counsel to Yahoo! Inc, to William Bordley, U.S. Marshals Service (Sept. 15, 2009), *available at* http://files.cloudprivacy.net/yahoo-price-list-letter.PDF.

124. *See* Yahoo!, *supra* note 71; Letter from Michael T. Gershberg, Attorney, Steptoe & Johnson LLP, to John Young, Cryptome, at (Dec. 2, 2009), *available at* http://www.eff.org/files/yahoo-demand.pdf. Yahoo!'s attempt to halt the spread of its price list was, by all estimates, a complete failure – the takedown led to significant media attention, both on the Internet and TV. *See* Zetter, *supra* note 102; *The Colbert Report: The Word – Spyvate Sector* (Comedy Central broadcast Dec. 16, 2009), *available at* http://www.colbertnation.com/the-colbert-report-videos/258582/december-16-2009/the-word---spyvate-sector.

of the Wisconsin State Public Defender.[125] Although I ignored their request, the file soon disappeared from the Wisconsin State Public Defender website, presumably after the office was also contacted by Facebook.

IV. ENCOURAGING COMPANIES TO COMPETE ON PRIVACY

As the preceding two sections demonstrate, there are several ways that telecommunications and Internet companies differ on practical privacy issues. If these firms chose to do so, they could actually compete on these meaningful differences, giving their customers another data point by which to compare their product offerings. However, for companies to be able to effectively compete on the degree to which they facilitate or resist government access to their customers' data, they must first be willing to publicly discuss their own policies. Simply put, for there to be effective competition on privacy, consumers (assisted by public interest groups and the media) need to be able to evaluate and compare each company's approach to government access.

Unfortunately, it is likely that most firms will vigorously resist any efforts to make such information public, particularly those firms that have adopted policies designed to assist the government (in some cases, for free and, in other cases, at a price). As such, any effort to force transparency in this area will likely occur in spite of most of the providers, rather than with their assistance. How can this information be freed and delivered to consumers to create a market for privacy?

This section will first briefly explore the existing surveillance statistics that have been made public, including those pursuant to specific statutory requirements and those that have been voluntarily provided by telecommunications and Internet providers. While these statistics are often useful for informing the general public about the extent of the government's surveillance activities, they do little to enable effective competition between individual providers.

The second half of this section will propose specific ways in which companies can be forced to provide meaningful information that will actually promote competition in the area of government access to end-user data.

125. Email from Jeff Wu, Facebook, to Author (Dec. 2, 2010, 4:31 PM) (on file with author).

A. GOVERNMENT COMPILED AGGREGATE SURVEILLANCE STATISTICS

Each year since 1997, the Administrative Office of the U.S. Courts has compiled and published a detailed report on the number of law enforcement wiretaps and other electronic intercepts that occurred at both the state and federal level in the previous year. The report is extraordinary in its high-level of quality[126] and in its detail in revealing the number of wiretaps requested and approved on a city/county scale, the kind of interception (phone, computer, pager, fax), the number of people whose communications were intercepted, the number of intercepted messages, the number of arrests and convictions that resulted from the interception, and the financial cost of the wiretap.[127]

Likewise, the DOJ is required at least once a year to submit several surveillance-related reports to Congress, including: a report regarding the use of pen registers and trap & trace devices by law enforcement agencies within the DOJ,[128] a report detailing the number of emergency disclosures of the contents of communications to the DOJ by ISPs,[129] a report detailing the number of applications made by the Government to conduct electronic surveillance and/or physical searches under the Foreign Intelligence Surveillance Act,[130] the number of "Section 215" requests for business records and tangible things for foreign intelligence purposes,[131] and the number of national security letters sent by the FBI.[132]

As detailed as the Wiretap Report is, it lacks one key bit of information: the names of the telecommunications carriers that received and complied with the intercept orders. The reports compiled by the DOJ similarly lack carrier information,

126. 145 Cong. Rec. 31,311 (1999) (statement of Sen. Leahy) ("The AO has done an excellent job of preparing the wiretap reports.").

127. 18 U.S.C. § 2519(2)–(3) (2006) (outlining what the intercepted communications report issued by the Administrative Office of the United States Courts must contain).

128. 18 U.S.C. § 3126 (2006).

129. 18 U.S.C. § 2702(d) (2006).

130. 50 U.S.C. § 1807 (2006); *see also* 50 U.S.C. § 1805(c)(1)(d) (2006).

131. *See* The USA Patriot Act, Pub. L. No. 107-56, § 215, 115 Stat. 272 (2001) (expanding the authority of the FBI to compel disclosure of certain business records under 50 U.S.C. § 1862(b)(1)).

132. 18 U.S.C. § 2709(e) (2006).

although this is less of an immediate problem because these reports are not even made available to the general public.

These reports may provide academics, privacy activists, and those in Congress with a partial sense of the scale of modern surveillance, at least at the federal level. However, they lack sufficient information to enable consumers to learn about the privacy practices of the companies to whom they entrust their private communications.

B. COMPANY PROVIDED SURVEILLANCE STATISTICS

Over the past few years, a small number of service providers have voluntarily published statistics regarding the extent to which they receive government requests. But as far as I am aware, no company has disclosed the extent to which it responds to or rejects those requests.

AOL was the first company to voluntarily disclose statistics, revealing to the New York Times in 2006 that it received 1000 requests per month.[133] In 2007, in response to a query from several members of Congress, Verizon provided detailed information regarding the requests it had received from government agencies, which averaged 90,000 per year.[134] In 2009, a representative from Facebook told Newsweek that it was receiving between ten to twenty requests from police per day.[135] Finally, in response to a copyright lawsuit in 2010, cable giant Time Warner revealed that it was receiving approximately 500 IP address lookup requests per month on average, nearly all of which come from law enforcement.[136] None of these companies have provided updated statistics since their initial disclosures.

---

133. Saul Hansell, *Online Trail Can Lead to Court*, N.Y. TIMES (Feb. 4, 2006), at C1 ("AOL, for example, has more than a dozen people, including several former prosecutors, handling the nearly 1,000 requests it receives each month for information in criminal and civil cases . . . . AOL says that only 30 of the 1,000 monthly requests it receives are for civil cases, and that it initially rejects about 90 percent of those, arguing that they are overly broad or that the litigants lack proper jurisdiction. About half of those rejected are resubmitted, on narrower grounds.").

134. Milch, *supra* note 1, at 4–5.

135. Nick Summers, *Walking the Cyberbeat*, NEWSWEEK (May 18, 2009), http://www.newsweek.com/id/195621.

136. Nate Anderson, *Time Warner Cable Tries to Put Brakes on Massive Piracy Case*, ARS TECHNICA, http://arstechnica.com/tech-policy/news/2010/05/time-warner-cable-tries-to-put-brakes-on-massive-piracy-case.ars (last updated May 2010).

In April 2010, Google announced its new Government Requests Tool, which reveals the number of government requests for user data that the company received between July 1, 2009 and December 31, 2009 broken down by country.[137] While the initial data set only covers a single six month period, Google pledged to update it twice per year going forward.[138] Google's release of this information instantly set a gold standard for transparency regarding government requests, far surpassing the previous efforts of its competitors. However, the company acknowledges that it is difficult to draw any conclusions from the limited data it has released:

> Requests may ask for data about a number of different users or just one user. A single request may ask for several types of data (for example, basic subscriber information or contents of emails) but be valid only for one type and not for another; in those cases, we disclose only the information we believe we are legally required to share. Given all this complexity, we haven't figured out yet how to categorize and quantify these requests in a way that adds meaningful transparency, but we plan to in the future.[139]

Until the release of this data, Google had long maintained a policy, like many other Internet companies, of not commenting on the number of requests it receives from government agencies.[140] 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.[141]

C. THE CURRENT STATISTICS ARE LACKING

Both the currently released official surveillance government statistics and the statistics voluntarily provided by

---

137. David Drummond, *Greater Transparency Around Government Requests*, THE OFFICIAL GOOGLE BLOG (Apr. 20, 2010, 11:04 AM), http://googleblog.blogspot.com/2010/04/greater-transparency-around-government.html.

138. *Id.*

139. *Transparency Report: FAQ*, GOOGLE.COM, http://www.google.com/governmentrequests/overview.html (last visited Oct. 15, 2010).

140. *E.g.*, Declan McCullagh, *How Safe Is Instant Messaging? A Security and Privacy Survey*, CNET NEWS (June 9, 2008, 4:00 AM), http://news.cnet.com/8301-13578_3-9962106-38.html; Ryan Singel, *Google, Microsoft Push Feds to Fix Privacy Laws,* WIRED (Mar. 30, 2010, 4:38 PM), http://www.wired.com/threatlevel/2010/03/google-microsoft-ecpa.

141. *See* Singel, *supra* note 140.

companies do little to enable consumers (and their proxies, such as public interest groups and the media) to determine which companies most effectively protect their customers' privacy. For example, Verizon received 88,000 government requests in 2006,[142] while Google received 3,000 requests over six months in 2009.[143] Does this mean that Verizon is a worse company for privacy or a better one? It is impossible to know. Missing from these numbers are details on the number of requests that each company refused to comply with, the number of voluntary disclosures, the amount of data that was eventually disclosed, and the number of customers whose data was delivered.

In order to stimulate a market for effective corporate resistance to government access, surveillance statistics need to reveal the activities and policies over which the carriers and providers actually have some degree of control. Specifically, information that could help consumers determine the extent to which their provider protects their privacy includes:

1. The number of emergency requests the company received, in which no subpoena, court order, or other legal process was submitted;
2. The number of emergency requests that the company rejected and the number with which it complied;
3. The number of instances in which the company refused to comply with a demand for information and went to court to quash the order;
4. The kind of information sought (prospective/real time or historical). In the event that logs or other stored information is sought, the age of the information disclosed to the government for each request; and
5. The number of instances in which the company had nothing useful to deliver due to data deletion policies or due to the use of encryption for which it does not have the key.

D. STATE GOVERNMENTS CAN FORCE THE DISCLOSURE OF SURVEILLANCE DATA

Over the last several decades, Congress has repeatedly expanded the ability for law enforcement and intelligence agencies to obtain individuals' private data, lowered the

142. Milch, *supra* note 1, at 5.

143. Ryan Singel, *Google: U.S. Demanded User Info 3,500 Times in 6 Months*, WIRED (Apr. 20, 2010, 1:12 PM), http://www.wired.com/threatlevel/2010/04/google-warrants-transparency/#comments.

evidentiary threshold required to get it, and permitted the large-scale collection of such sensitive information without judicial oversight.

Because of this consistent trend, I hold the rather pessimistic view that Congress is unlikely to pass any legislation aimed at encouraging companies to say no to government agencies' requests for customers' data. However, the federal government is not the only avenue for legislative action —often, change starts with the states.[144]

For example, over the past several years, forty-six states have adopted data breach statutes, all following California's lead in 2003.[145] This is, of course, a great example of states acting to protect their citizens when the federal government is unwilling or unable. Furthermore, these benefits are not limited to just the residents of the states that pass such laws. For example, in 2004, data broker ChoicePoint suffered a significant data breach.[146] Soon enough, ChoicePoint admitted that it had suffered a breach that impacted individuals from across the country.[147]

States can play a significant role in shining light upon companies' surveillance practices. Furthermore, Americans from all fifty states, as well as consumers around the world, can free-ride and receive similar benefits, even if just one or two states act.

As such, I present the following policy proposals, which could be implemented by any state (although, ideally by California, given how many Internet service and application providers are based there):

---

144. *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J. dissenting) ("It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

145. *State Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES, http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx (last updated Apr. 12, 2010).

146. Gary Rivlin, *Keeping Your Enemies Close*, N.Y. TIMES (Nov. 12, 2006), *available at* http://www.nytimes.com/2006/11/12/business/yourmoney/12choice.html?_r=1&ref=choicepoint-inc.

147. *Id.*

1. Require that companies disclose their data retention policies, including the details and any limitations of the methods used for data deletion or anonymization policies.
2. Require that companies disclose their policy for the voluntary disclosure of information, including the standards used to evaluate emergency situations.
3. Require that companies calculate statistics on the number of requests they receive from law enforcement each year and the number of individuals or accounts whose information is requested, the legal process accompanying the request, the number of times the company refuses to or discloses the information sought, and the type of user data sought and disclosed. For these statistics, the companies should disclose the relevant numbers for the state, as well as a nationwide total.
4. Require that companies disclose the amount of money, if any, they charge the government for responding to requests for user data and the degree to which the company makes a profit from such disclosures.

Should at least one state mandate such disclosures, those companies that go out of their way to assist the government would be clearly identified, as well as those that put their customers' privacy first. At that point, consumers would be free to include this information in their purchasing decisions, and hopefully, spur a real market for privacy.

E. A ROLE FOR THE FEDERAL TRADE COMMISSION

> "Consumers need to understand how the information they share will be used, so that they can make informed decisions about whether to share it in the first place."[148]

The United States is unique among western countries in that its primary privacy regulator, the FTC, is entirely focused on privacy violations by companies but not the government. Contrast this to Europe and Canada, where privacy commissioners are free to comment on matters of government surveillance. For example, in the same month, Canada's Privacy Commissioner condemned the proposed rollout of full-body scanners at airports[149] and launched an investigation into

148. David Vladeck, Dir., FTC Bureau of Consumer Prot., Remarks at New York University: Promoting Consumer Privacy: Accountability and Transparency in the Modern World (Oct. 2, 2009), *available at* http://www.ftc.gov/speeches/vladeck/091002nyu.pdf.

149. Jennifer Stoddart, Op-Ed., *Airport Security Scanners Must Respect Privacy, Privacy Commissioner Insists*, OFFICE PRIVACY COMM'R CAN., Jan. 2010, http://www.priv.gc.ca/media/nr-c/2010/op-ed_100107_e.cfm.

Facebook's privacy flaws.[150] Contrast this to the United States, where, for several years, every privacy activist, public interest group, and civil liberties-inclined member of Congress railed against the National Security Agency's warrantless wiretapping program—yet, the FTC did not comment on, or involve itself in, the matter. The reason, of course, was the FTC's strict mandate to regulate unfair and deceptive business practices. The activities of the NSA, the FBI, and the DOJ, no matter how illegal, are strictly outside the FTC's regulatory authority.

Even though the FTC cannot stop other government agencies from intruding upon or violating the privacy of Americans, it may be able to play a role in regulating the companies that go out of their way to assist government agencies in their data collection activities, at least when those firms simultaneously promise to protect their users' privacy.

Since the FTC's first privacy cases in 2004, a consistent enforcement hook for the agency has been the privacy policies that both the Children's Online Privacy Protection Act (COPPA)[151] and California's Online Privacy Protection Act of 2003 (OPPA)[152] required companies to post on their websites. If a company claims to do something in its privacy policy and it does not do so (or does not do so sufficiently), the FTC is able to act.

The most relevant of the FTC's privacy cases is the *Tower Records* settlement from 2004.[153] In that case, the company's privacy policy claimed that "TowerRecords.com takes steps to ensure that your information is treated securely . . . [and] [o]nce we receive your transmission, we make our best effort to ensure its security on our systems."[154] When the company failed to protect end users' data from hackers, the FTC argued that Tower had failed to:

> [I]mplement appropriate checks and controls on the process of writing and revising Web applications; adopt and implement policies and

150. Press Release, Office of the Privacy Comm'r of Canada, Privacy Commissioner Launches New Facebook Probe (Jan. 27, 2010), *available at* http://www.priv.gc.ca/media/nr-c/2010/nr-c_100127_e.cfm.

151. 15 U.S.C. §§ 6501–6506 (2006).

152. CAL. BUS. & PROF. CODE §§ 22575–22579 (Deering 2010).

153. *See* Complaint, *In re* MTS, Inc., 137 F.T.C. 444 (May 28, 2004) (No. 032-3209).

154. *Id.* at 454.

> procedures regarding security tests for its Web applications; and provide appropriate training and oversight for their employees regarding Web application vulnerabilities and security testing."[155]

According to the Commission, the disparity between the security failure and the assurances given in Tower's privacy policy constituted "unfair or deceptive acts or practices" in violation of the Federal Trade Commission Act.[156]

As the proceeding sections of this article have demonstrated, companies have a significant amount of flexibility in the way that they design their systems and in the interpretations of ECPA that they adopt. Furthermore, as the quotes and facts included earlier demonstrate, Google, Microsoft, Verizon, and AT&T have all opted to put their desire to assist the government above their customers' privacy interests. However, these firms also make prominent statements about their commitment to protecting their customer privacy. No mention is made in their respective privacy policies about their belief that the government's interest in conducting investigations comes first.

These firms, as well as others in the industry, should be free to design their products in any way they wish, and, where the law permits, they should be free to voluntarily assist the government in any way they choose. What they should not be permitted to do, however, is to proclaim their commitment to protecting their customers' privacy and then actively subvert it by designing their systems to put the government's interests first.

The bold promises by these companies mislead consumers about a material aspect of each firms' data and privacy policies, and the degree to which the consumers' information is protected. As such, the FTC can and should stop these companies from falsely claiming to protect their customers' privacy.

I acknowledge that the FTC's involvement in this area would be controversial and fraught with political risk, a very real concern for an agency that has had its budget slashed by Congress in the past in response to a belief by many in Congress that it had wandered beyond its mandate.[157]

---

155. *Id.* at 448.

156. *Id.* at 449.

157. *See, e.g.*, Haoran Lu, *Presidential Influence on Independent Commissions: A Case of FTC Staffing Levels*, 28 PRESIDENTIAL STUD. Q., 51, 54–56.

As such, my proposal is only that the FTC prohibit these firms from making unqualified statements about their commitment to user privacy and not that the FTC force these firms to actually adopt privacy enhancing technologies and policies. These companies should simply have to tell their customers the truth—that their privacy is not as important as maintaining the government's investigative abilities.

Were the FTC to enforce such truth in privacy statements, it could have a significant stimulating effect on the market for privacy enhancing services, and consumers might for the first time be able to easily evaluate potential service providers based on these statements. There are, of course, many Americans who seem to support the government's desire to freely spy on its citizens, and these consumers would be able to easily identify companies whose policies match their own beliefs. On the other hand, consumers who value their privacy and civil liberties would be able to identify the service providers who are most committed to protecting their private information from government intrusion.

V. CONCLUSION

Although many companies claim to value and protect privacy, this article clearly demonstrates that this is simply not the case, at least with regard to government access to user data. Although companies have significant flexibility in designing their products to be resistant to the government, few take the steps to do so; yet, most continue to tout their commitment to protecting user data.

As a result of this lack of accurate information about companies' practices, there is no functioning market for this kind of privacy. Consumers have no way to evaluate each firm's practices and, as such, may entrust information to these firms that they otherwise might not have had they known the circumstances in which the company might voluntarily provide it to the government.

If a healthy market for privacy existed, consumers would be able to vote with their dollars. The large numbers of Americans who are willing to sacrifice their civil liberties in the government's never-ending fight against terror would be able to steer their dollars to firms that share that belief. On the other hand, Americans who value their privacy and distrust the government would be able to easily determine which firms

match their own beliefs. Ideally, such transparency would push companies to follow consumer preferences—either for more disclosure to the government or less. Without action, we will never get such transparency and competition.