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

*Christopher Soghoian***

Today, when consumers evaluate potential telecommunications, Internet service or application providers – they are likely to consider several differentiating factors: The cost of service, the features offered as well as the providers' reputation for network quality and customer service. The firms' divergent approaches to privacy, and in particular, their policies regarding law enforcement and intelligence agencies' access to their customers' private data are not considered by consumers during the purchasing process – perhaps because it is practically impossible for anyone to discover this information.

A naïve reader might simply assume that the law gives companies very little wiggle room – when they are required to provide data, they must do so. This is true. However, companies have a huge amount of flexibility in the way they design their networks, in the amount of data they retain by default, the exigent circumstances in which they share data without a court order, and the degree to which they fight unreasonable requests. As such, there are substantial differences in the privacy practices of the major players in the telecommunications and Internet applications market: Some firms retain identifying data for years, while others retain no data at all; some voluntarily provide government agencies access to user data - one carrier even argued in court that its 1st amendment free speech rights guarantee it the right to do so, while other companies refuse to voluntarily disclose data without a court order; some companies charge government agencies when they request user data, while others disclose it for free.

** Ph.D. Candidate, School of Informatics and Computing, Indiana University. Email: csoghoian@gmail.com. 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 both 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, Judge Stephen Wm. Smith, Joris Van Hoboken, as well as several anonymous individuals for their assistance and feedback on the theories presented in this article.

As such, a consumer's decision to use a particular carrier or provider can significantly impact their privacy, and in some cases, their freedom.

Many companies profess their commitment to protecting their customers' privacy, with some even arguing that they compete on their respective privacy practices. However, none seem to be willing to disclose, let alone compete on the extent to which they assist or resist government agencies' surveillance activities. Because information about each firm's practices is not publicly known, consumers cannot vote with their dollars, and pick service providers that best protect their privacy.

In this article, I focus on this lack of information and on the policy changes necessary to create market pressure for companies to put their customers' privacy first. I outline the numerous ways in which companies currently assist the government, often going out of their way to provide easy access to their customers' private communications and documents. I also highlight several ways in which some companies have opted to protect user privacy, and the specific product design decisions that firms can make that either protect their customers' private data by default, or make it trivial for the government to engage in large scale surveillance. Finally, I make specific policy recommendations that, if implemented, will lead to the public disclosure of these privacy differences between companies, and hopefully, create further market incentives for firms to embrace privacy by design.

Contents

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] "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 a chief privacy officer.[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

---

[1] http://markey.house.gov/docs/telecomm/Verizon_wiretaping_response_101207.pdf

[2] http://www22.verizon.com/about/privacy/letter/

[3] http://www.google.com/privacy_faq.html

[4] http://googleblog.blogspot.com/2008/07/what-comes-next-in-this-series-13-33-53.html

[5] http://news.zdnet.com/2100-9595_22-394881.html

[6] http://go.microsoft.com/?linkid=9688090

[7] This is likely because of California's Online Privacy Protection Act of 2003 - Business and Professions Code sections 22575-22579. "This law requires operators of commercial web sites or online services that collect personal information on California residents through a web site to conspicuously post a privacy policy on the site and to comply with its policy. The privacy policy must, among other things, identify the categories of personally identifiable information collected about site visitors and the categories of third parties with whom the operator may share the information." http://www.privacy.ca.gov/privacy_laws.htm

[8] "Between 1995 and 2010, corporate privacy management in the U.S. has undergone a profound transformation. Following the lead of the financial and health sectors, thousands of companies have created Chief Privacy Officer positions, a development often accompanied by prominent publicity campaigns. A professional association of privacy professionals boasts over 6,500 members, and offers information privacy training and certification. A robust privacy law practice has arisen to service the growing group of professionals and assist them in assessing and managing privacy." Bamberger, Kenneth A. and Mulligan, Deirdre K., Privacy on the Books and on the Ground. Stanford Law Review, Vol. 63, 2010

privacy,[9] most visibly, the major search engines that have repeatedly one-upped each other, adopting ever-more privacy-protecting data retention policies.[10]

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 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 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 user privacy," the company has argued in court that it has a 1st amendment right to voluntarily provide information about its customers' private communications to the National Security Agency.[12] 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.

Google has made bold statements about the "trust our users place in us, and our responsibility to protect that privacy." The company also has a YouTube privacy channel with nearly 50 videos describing

---

[9] "I'll just be really clear: We compete on privacy. We do that in terms of trying to develop the best possible products that are privacy sensitive. We do that because we have an entire team of engineers specifically dedicated to privacy, and a cross-functional group that meets every week that involves everyone from engineers to policy people to legal people to talk about the biggest issues in privacy. We absolutely compete in this space." (Statement of Google Counsel Nicole Wong, http://www.mediabistro.com/baynewser/privacy/google_privacy_chief_we_absolutely_compete_on_privacy_150406.asp)

[10] Search engines are in an arms race to offer better privacy protections to the users." Katherine Mangu-Ward, Reason, http://reason.com/blog/2007/08/13/search-engines-compete-on-priv. "With Google taking some hits over its data retention practices, its competitors are hoping that they can use the privacy issue to their advantage." Techdirt. http://techdirt.com/articles/20070723/100944.shtml "After years of insisting that they should be trusted to keep users' search histories indefinitely, search engines are suddenly competing to limit data retention." http://www.newsfactor.com/story.xhtml?story_id=010000TXY69E

[11] See generally Mulligan, page 26.

[12] "The gravamen of plaintiffs' records claims is that defendants allegedly communicated `information' about them to the government— namely, that a call was placed from a certain telephone number to another number. Communicating such factual information to the government would be speech that is fully protected by the First Amendment." http://www.eff.org/files/filenode/att/verizonmemmtd.pdf

the privacy features built into its products and one that promises that the company "makes privacy a priority in everything we do."[13] However, absent from the company's YouTube privacy channel is a copy of the October 2009 National Public Radio interview with Google CEO Eric Schmidt, in which he revealed that one of the main reasons the company retains identifying user log data is so that it may deliver it to the government.[14]

Finally, Microsoft has pledged that it takes its "customers privacy seriously." 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."[15] 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've 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.

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 I 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

---

[13] http://www.youtube.com/watch?v=5fvL3mNtl1g

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

[15] http://www.nytimes.com/2007/07/23/technology/23microsoftweb.html

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 II 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 reveal the extent to which they are willing to fight the government. This section sheds a significant amount of light on this subject, and in particular, reveals several novel, privacy-preserving interpretations of ECPA that some service providers have adopted.

Finally, Section III 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, and this section will propose several ways to fix this fundamentally broken market.

PART I: Engineering and policy decisions can significantly restrict government access to data

Technology firms in the United States are largely free to design their products and networks in any way they wish to do so, at least with regard to the extent to which privacy enhancing technologies are included.[16] Outside of the financial and common carrier telephone industries,[17] there are no data retention laws, and the few other regulations are focused on making sure that companies sufficiently protect their customers' data from improper access – by rogue insiders, as well as hackers and other criminals.

Email, search engine, and broadband Internet service providers 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 to deliver to the government.

This section will explore several ways that companies' engineering design decisions and data storage policies differ, and analyze the impact that such decisions have on their customers' privacy. 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.

Leaking IP addresses in email headers

Several of the big free web mail providers intentionally leak their users' IP addresses to anyone that their subscriber contacts by email. This engineering decision, something not required by technical

[16] "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,' United States v. New York Telephone, 434 U.S. 159, 177 (1977), 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." (http://www.askcalea.net/docs/hr103827.pdf - CALEA legislative history).

[17] 47 C.F.R. § 42.6 Retention of telephone toll records. "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."

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 user 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.[18]

When a user of Microsoft's Hotmail or Yahoo! Mail services sends an email 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 IP address.

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

> X-Originating-IP: [68.48.136.114][19]

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 voluntary 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.[20]

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.

Starting in at least 2006, when a Facebook user commented on another user's profile, left a comment on their "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:

---

[18] "[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." http://www.onthemedia.org/transcripts/2010/04/23/05

[19] http://postmaster.live.com/FAQ.aspx

[20] https://mail.google.com/support/bin/answer.py?hl=en&answer=26903

> Received: from zuckmail ([68.48.136.114]) by hs.facebook.com with HTTP[21]

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:[22]

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

News of Facebook's IP address header spread across Internet blogs and forums in May 2010. In response, the company quickly changed the header, so that the user's real IP address was no longer leaked.[23]

The privacy impact of leaking user IP addresses

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, 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 US 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 can then go directly to the broadband Internet service provider 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 force the police to seek a court order if they sought to delay such notice.[24]

---

[21] 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 and http://supersat.livejournal.com/71945.html

[22] http://www.digitalthreat.net/2010/05/facebook-notifications-leak-ip-addresses/

[23] http://www.binint.com/2010/05/facebook-leaks-ip-addresses.html

[24] See 18 USC 2705

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 come from a 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, Myanmar, Zimbabwe or some other oppressive regime is using their US 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 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.

Community of interest databases

In 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."[25] However, the government soon took an interest in the ability to sift through the telecom giant's vast databases.

In 2007, it was revealed that 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. These records might include an analysis of which people the targets called

[25] Cortes, C., Pregibon, D., and Volinsky, C. 2001. Communities of Interest. In Proceedings of the 4th international Conference on Advances in intelligent Data Analysis (September 13 - 15, 2001). F. Hoffmann, D. J. Hand, N. M. Adams, D. H. Fisher, and G. Guimarães, Eds. Lecture Notes In Computer Science, vol. 2189. Springer-Verlag, London, 105-114.

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.[26]

A subsequent investigation by the Inspector General of the Department of Justice found that these powers had been widely abused by the FBI. 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.[27]

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." 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.[28]

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. By not deploying a similar system, Verizon effectively protected its customers' privacy against fishing expeditions and other large-scale requests for information.

Proactive searches for child pornography

US federal law requires that Internet Service Providers immediately notify the appropriate authorities when they detect or otherwise learn about the presence of child pornography on their servers.[29] In order to comply with the law, most large Internet companies, particularly those that host user

[26] http://www.nytimes.com/2007/09/09/washington/09fbi.html?pagewanted=1&_r=1

[27] http://www.justice.gov/oig/special/s1001r.pdf at page 61 (original numbering).

[28] "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." http://markey.house.gov/docs/telecomm/Verizon_wiretaping_response_101207.pdf (page 13)

[29] See: 18 USC 2258A.

generated images and videos, review content that has been flagged by their users, or other third parties.[30]

The law does not, however, require that ISPs proactively seek out such materials by automatically analyzing their customers' communications. Nevertheless, at least one Internet Service Provider has 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 Center (NCMEC) as required by law.

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 transmission . . . of child pornography on its systems."[31]

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-government NCMEC, few will go on record to air such complaints.[32]

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

[30] "tech giants like Microsoft, Yahoo and MySpace, a division of the News Corporation, all outsource some amount of content review….YouTube, a division of Google, is an exception… Flagged videos are then sent for manual review by YouTube-employed content moderators…. Facebook, the dominant social network with more than 500 million members around the world, has relied on its users to flag things like pornography or harassing messages. That material is reviewed by Facebook employees." https://www.nytimes.com/2010/07/19/technology/19screen.html

[31] U.S. v. Richardson, 2010 WL 2340233 (U.S. Court of Appeals for the 4th Circuit 2010)

[32] "Over the past several weeks, I've spoken to a number of experts in the field of Internet law and policy. Many of those have strong feelings about NCMEC, but due to the extremely sensitive nature of the child pornography issue, few would go on record to voice their criticism." http://news.cnet.com/8301-13739_3-10118923-46.html

the extent to which they can be compelled to use it.[33] 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.[34]

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

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, increasingly, some firms are also encrypting users' data in storage, so that no one other than the end user (including the service provider) can access the data.

Telecommunications carriers and technology firms in the United States are legally free to add encryption capabilities to their products.[35] 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 other "information necessary to decrypt the communication," it has no legal obligation to decrypt its users' data, or otherwise ensure

[33] Telecommunications lawyer Al Gidari describes this as, "if you build it, they will come".

[34] 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.

[35] CALEA legislative history (http://www.askcalea.net/docs/hr103827.pdf) "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."

the government's ability to decrypt any subscriber encrypted communication. 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.[36]

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 Internet Service Providers using Deep Packet Inspection hardware in order to deliver behaviorally targeted advertising[37], and it also 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.

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.[38] However, a couple cloud computing firms have opted to encrypt user data in 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, 38 industry and academic experts from the fields of computer security, privacy and law (lead by this author) wrote an open letter to Google's Chief Executive Officer to chastise the company for its lack of

---

[36] 47 USC 1002 (b)(3): "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."

[37] See generally: Paul Ohm, The Rise and Fall of Invasive ISP Surveillance, 2009 University of Illinois Law Review 1417 (2009).

[38] "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." Predrag Klasnja et al., *"When I am on Wi-Fi, I am Fearless:" Privacy Concerns & Practices in Everyday Wi-Fi Use*, In CHI '09: Proceedings of the 27th international conference on Human factors in computing systems 1993 (2009), *available at* http://www2.seattle.intel-research.net/~jjung/FormativeUserStudy4CHI.pdf. "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.." Letter from Jacob Appelbaum et al. to Google CEO Eric Schmidt (June 16, 2009), *available at* http://www.cloudprivacy.net/letter/.

default transport encryption.[39] Seven months later, the company enabled HTTPS encryption by default for all of its Gmail users, although users of its Docs, Spreadsheets and Calendar services must still proactively connect via a HTTPS based URL if they wish to have their connections protected by SSL.[40] Similarly, in May of 2010, the company began to offer SSL encrypted search (although this, like encryption for its Docs, Spreadsheets and Calendar services remains disabled by default for now[41]), making it the first major search engine to do so.[42]

Following Google's lead, or perhaps feeling increased pressure from consumer protection regulators,[43] Microsoft announced in May 2010 that it too would be offering SSL protection for its popular Hotmail service later in the year, although not enabled by default.[44]

---

[39] "Google is putting millions of users at risk of fraud from hackers and needs to enable encryption by default on its most popular web apps, including Gmail and Google Docs, a gaggle of security researchers told the search giant Tuesday in an open letter." Ryan Singel, *Encrypt the Cloud, Security Luminaries Tell Google – Update*, WIRED, June 16, 2009, http://www.wired.com/threatlevel/2009/06/google_ssl/; *see also* Appelbaum, *supra* note 61.

[40] "In 2008, we rolled out the option to always use https — encrypting your mail as it travels between your web browser and our servers. Using https helps protect data from being snooped by third parties, such as in public wifi hotspots. We initially left the choice of using it up to you because there's a downside: https can make your mail slower since encrypted data doesn't travel across the web as quickly as unencrypted data. Over the last few months, we've been researching the security/latency tradeoff and decided that turning https on for everyone was the right thing to do."

Posting of Sam Schillace to The Official Gmail Blog, Default HTTPS Access For Gmail, http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html (January 12, 2010).

[41] "A Google spokesman also indicated it plans to make SSL encryption the default for search. 'We hope to expand the functionality once we better understand how it affects users' search experience,' the spokesman told us. 'We expect that encrypted SSL search will slow down Google searches by a small degree, and we don't like the idea of rolling this out to everyone before we're able to test the performance effects and gather feedback from our users.'" http://www.theregister.co.uk/2010/05/21/google_search_ssl_encryption/

[42] "And today we're gradually rolling out a new choice to search more securely at https://www.google.com. When you search on https://www.google.com, an encrypted connection is created between your browser and Google. This secured channel helps protect your search terms and your search results pages from being intercepted by a third party on your network." http://googleblog.blogspot.com/2010/05/search-more-securely-with-encrypted.html.

[43] "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." FTC Commissioner Pamela Jones Harbour, Remarks Before Third FTC Exploring Privacy Roundtable Washington, D.C., March 17, 2010 http://www.ftc.gov/speeches/harbour/100317privacyroundtable.pdf

The 38 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 through the assistance of major telecom carriers who have given intelligence agencies access to their backbone networks.[45]

Whatever the motivation for the switch to SSL, Google's decision had a very real impact upon 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. [46] 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.[47] Yahoo! and Hotmail, neither of which offers encryption by default, were not blocked by the Iranians.

Storage encryption

Cloud-based services do not, by their very nature, have to store their users' data in the clear, and thus put the privacy of their users at risk. Consider, as an example, the Firefox Sync add-on for the Firefox web browser.[48] This tool enables users to keep their bookmarks, browsing history, saved passwords, and cookie synchronized across multiple computers. The tool includes support for the Firefox mobile phone browser, allowing users to bookmark a web page at home and then later view it later on in the day from their phone.

Like all cloud services, The Mozilla Corporation (which makes Firefox and Firefox Sync) 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

---

[44] "In addition to providing SSL encryption at login for all accounts, the new Hotmail will soon support the option to maintain SSL encryption between you and our servers during your entire Hotmail session." http://www.liveside.net/main/archive/2010/04/30/windows-live-hotmail-wave-4-to-get-exchange-activesync-support-full-session-ssl-and-more.aspx

[45] For example, "According to current and former intelligence officials, the spy agency now monitors huge volumes of records of domestic emails and Internet searches as well as bank transfers, credit-card transactions, travel and telephone records." http://online.wsj.com/article/SB120511973377523845.html

[46] http://www.nytimes.com/2010/02/11/world/middleeast/11tehran.html?partner=rss&emc=rss

[47] "Some communications experts believe that the authorities' efforts to block Gmail could be related to Google encryption, which prevents the government from reading e-mail. Yahoo and Hotmail have not been similarly affected, one monitor said." http://www.nytimes.com/2010/02/11/world/middleeast/11tehran.html?partner=rss&emc=rss

[48] See: http://mozillalabs.com/weave/

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.”[49] As a result, the data that Sync users store on Mozilla’s servers is encrypted with a key created by that user, which is not shared with anyone else. Mozilla simply provides the cloud-based storage, but is unable to peek at its users’ stored passwords and browsing history. 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 make use of encryption to securely store users’ data in the cloud. Over the past several years, numerous companies have started to offer cloud based backup solutions – enabling users to automatically store their personal documents and other important files online.[50] However, of all these services, SpiderOak has opted to build strong encryption into their product by default.[51] The company describes itself as a "zero knowledge backup provider,” arguing that “we do not know anything about the data that you store on SpiderOak -- not even your folder or filenames. On the server we only see sequentially numbered containers of encrypted data.” Other than its strong encryption feature, the service is remarkably similar to the numerous other products in the online backup market.[52]

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 because 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 you cannot look at.[53] If these firms do eventually decide to offer encrypted cloud based storage, it is likely to first be to the enterprise customers who are charged a yearly fee to use the firms’ services.

---

[49] Mozilla Wiki, Overview of OAuth for Weave, https://wiki.mozilla.org/Labs/Weave/OAuth.

[50] These include Dropbox, Box.net, Sugarsync, Elephantdrive, and Microsoft Live Mesh.

[51] https://www.spideroak.com

[52] https://spideroak.com/engineering_matters#true_privacy and https://spideroak.com/faq/does_spideroak_use_encryption_when_storing_and_transferring_data

[53] “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.” http://jthtl.org/content/articles/V8I2/JTHTLv8i2_Soghoian.PDF at 37.

Data retention policies

The decision to delete data is often one of the most effective ways a company can preserve the privacy of its customers. There are of both direct and indirect costs for keeping data – the cost of the storage technology (hard disks, backup tapes) shrink every year, making it cheaper and cheaper to retain data, however, the increasing costs of PII 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.[54]

As such, most technology providers and communications carriers now have established data retention policies, which 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.

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 can be 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 24 month period. 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.[55] In contrast,

---

[54] See: "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." http://www.networkworld.com/news/2010/012510-data-breach-costs.html

"Data protection laws have turned Personal Information ("PI") into the intangible equivalent of toxic waste" http://www.engr.washington.edu/epp/infosec/presentations/Sep%2016%20data%20as%20toxic%20asset%20presentation%20as%20sent%20V2.ppt

"We should treat personal electronic data with the same care and respect as weapons-grade plutonium - it is dangerous, long-lasting and once it has leaked there's no getting it back" http://www.guardian.co.uk/technology/2008/jan/15/data.security

[55] "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. " (Paul Taylor, Electronic Surveillance Manager, Sprint Nextel, speaking at the ISS World Conference, Washington DC,

both T-Mobile and Cricket Communications use a Network Address Translation (NAT) based infrastructure,[56] in which all customers from a region appear to use one of a handful of IP addresses. As such, the companies are unable to reveal after the fact which particular customer was responsible for traffic originating from their network.[57]

As a result of these policies, a Sprint Nextel customer can be later tracked down based on an anonymous comment left on a blog, or a 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. Based on the handbooks that have been leaked thus far, I have been able to create the table below. Clearly, many companies are missing from the table – but compared to what was known one year ago, this is a great step in the right direction (even if it wasn't accomplished with the assistance or consent of the firms whose policies have been revealed).

October 13, 2009. Audio available at http://www.eff.org/files/soghoian-surveillance-dump.zip at approximately 105:45).

[56] Fixme – add footnote that describes NAT

[57] "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." (Janet A. Schwabe, Subpoena Compliance Manager, Cricket Communications speaking at the ISS World Conference, Washington DC, October 13, 2009. Audio available at http://www.eff.org/files/soghoian-surveillance-dump.zip at approximately 105:00).

"[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."(Gavin Pinchback, Director, Law Enforcement Relations, T-Mobile USA, speaking at the ISS World Conference, Washington DC, October 13, 2009. Audio available at http://www.eff.org/files/soghoian-surveillance-dump.zip at approximately 108.09).

Company	IP Address Login Data Retained	Account Registration Information Retained
Microsoft	60 days[58]	Life of account.
Yahoo	6 months[59]	Life of account + 90 days after deletion.
AOL	60-90 days[60]	*Unknown*
M ySpace	1 year[61]	Life of account + 1 year after deletion.
Facebook	90 days[62]	Until changed by user.
Time Warner Cable	6 months[63]	Unknown

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, 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 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 30 days or less that the data was

[58] http://cryptome.org//isp-spy/microsoft-spy.zip

[59] http://cryptome.org/isp-spy/yahoo-spy.pdf

[60] http://cryptome.org/isp-spy/yahoo-spy.pdf

[61] http://cryptome.org/isp-spy/myspace-spy.pdf

[62] http://cryptome.org/isp-spy/myspace-spy.pdf

[63] "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 could not be answered." http://arstechnica.com/tech-policy/news/2010/05/time-warner-cable-tries-to-put-brakes-on-massive-piracy-case.ars

retained two years ago. [64] 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 90 days. In 2007, the company expanded its logging of this data to 1 year. Facebook logged IP addresses for 30 days in 2007, but by 2008, the company had opted to keep the logs for 90 days.[65]

These social network sites did not publicly announce a change of policy, nor did they update their privacy policies to reflect what a rather significant shift (likely because the privacy policies did not list the original data retention period, let alone the new one). Instead, the only mention of it was 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 stored] United States communications records (including telephone and Internet records)."[66] Needless to say, neither Verizon nor AT&T, two of

---

[64] Cellular providers tend not to retain moment-by-moment logs of when each mobile device contacts the tower, in part because there's no business reason to store the data, and in part because the storage costs would be prohibitive. They do, however, keep records of what tower is in use when a call is initiated or answered--and those records are generally stored for six months to a year, depending on the company.

Verizon Wireless keeps "phone records including cell site location for 12 months," Drew Arena, Verizon's vice president and associate general counsel for law enforcement compliance, said at a federal task force meeting in Washington, D.C. last week. Arena said the company keeps "phone bills without cell site location for seven years," and stores SMS text messages for only a very brief time.

Gidari, the Seattle attorney, said that wireless carriers have recently extended how long they store this information. "Prior to a year or two ago when location-based services became more common, if it were 30 days it would be surprising," he said. http://news.cnet.com/8301-13578_3-10451518-38.html

[65] Law enforcement handbooks for MySpace and Facebook on file with author.

[66] The FBI requests $5,358,000 to partner with the telecommunications industry to access lawfully requested telephone records for CT investigations. The goal of the TDCC is to provide near real- time access to United States communications records (including telephone and Internet records) needed for CT investigations. Currently, the FBI has partnered with three long-distance carriers. The requested funding would allow for the continuation of telecommunications industry participation at the current level of three carriers, providing access to land-line phone call, calling card, cellular phone call, and Internet communications records, all delivered in an electronic format that can be exploited immediately to help resolve terrorist threats. This request is based on historical experience working with existing partners. The cost per telecommunications company currently participating in the TDCC is approximately $1,800,000. A recurring budget level of $5,358,000 would allow for the continued participation of three telecommunications companies to participate in the TDCC. …

The requested funding will allow for the development of data storage and retrieval systems by each contractor, accessible only by the contractor, for at least two years' worth of network calling records. In addition, each contractor would provide a dedicated on-site employee to process the exigent lawful requests for data.

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 this relationship to monetize their data, and increase the ease with which it could be disclosed to FBI agents.

The impact of zero data retention policies – or unintended consequences of the copyright lobby

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

In April 2009, Sweden enacted a controversial law which grants copyright holders the authority to request the personal details of alleged infringers from Internet Service Providers. The response from consumers was swift: Swedish Internet traffic dropped by over thirty percent starting the day that the new law came into effect.[67] This clear demonstration of consumer's privacy fears then lead to rapid competition in the market for privacy-preserving services.

Within weeks, three of Sweden's Internet Service Providers had 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 that "it's a strong wish from our customers, so we decided not to store information on customers' IP numbers."[68]

The adoption of these zero data retention policies has 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 is has become much harder for the police to trace and identify criminal suspects.[69]

Without dedicated funding for this initiative and contractors to pull together data for the FBI, market demands on these companies only require them to keep records online (quickly available) for the short period required to collect bills. After billing periods have passed, records are archived; therefore, retrieving them in a time frame shorter than several weeks is not possible.

http://www.wired.com/images_blogs/threatlevel/files/communicationsexploitationoffice08budget.pdf

[67] 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. *Piracy Law Cuts Internet Traffic*, BBC NEWS, Apr. 2, 2009, http://news.bbc.co.uk/2/hi/technology/7978853.stm.

[68] 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.

[69] "It is a major concern, for example, when minors are exploited for sexual purposes via the Internet but we can not trace the perpetrators because logging information is missing." http://torrentfreak.com/police-say-anti-

Outside of Sweden, the threat of copyright lawsuits has also almost singlehandedly created a growth industry in commercial anonymous Virtual Private Network (VPN) providers, who openly advertise zero log retention polices, through which users of peer-to-peer software can download content without fear of being identified.[70] Of course, these services' zero log retention policies thwart investigations by law enforcement agencies, in addition to just RIAA lawyers.

piracy-law-makes-catching-criminals-harder-100517/ and http://sverigesradio.se/sida/artikel.aspx?programid=1646&artikel=3701178

[70] "No provider logs" http://www.flashvpn.com/; "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." http://www.yourprivatevpn.com/?q=en/faq_en; "For the privacy and anonymity of our members we have disabled logging." http://www.perfect-privacy.com/faq.html "Traffic Logging... Right now, your ISP can see everything you do. You're about as untraceable as a stencil. Every torrent, every video, every piece of porn you look at can be stored in a nice big file. You're an open book to your providers and anyone else who wants a look. Do you want to put up with that? Of course not. We'll make your traffic completely transparent. Anonymity is our business." http://torrentfreedom.com/

PART II: Strict interpretations of the law can also restrict government access to data

The Electronic Communications Privacy Act (ECPA) details the instances in which telecommunications carriers and Internet service providers can and cannot disclose their customer's 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 isn't much that the company can do, other than disclosing 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.

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."

There has been considerable debate about the definition of the term "electronic storage," as the Department of Justice has taken the position that once an email message has been opened, it is no longer in electronic storage, and thus, can be divulged pursuant to a subpoena or 2703(d) order. The government's narrow interpretation of "electronic storage" was rejected by the Ninth Circuit in *Theofel v. Farey-Jones,*[71] in which the court held that email messages continue to be in "electronic storage" regardless of whether they had been previously accessed.[72] As such, prosecutors within the Ninth Circuit are bound by *Theofel*. However, the Department of Justice 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.[73]

Many large internet service providers take a different position. Some have argued that since their corporate headquarters are located within the Ninth Circuit, they must adhere to the *Theofel* precedent.[74] Others have simply argued that they believe that *Theofel* is the correct interpretation of

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

[72] See generally: Kerr, Orin S., A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It. George Washington Law Review, 2004

[73] http://www.justice.gov/criminal/cybercrime/ssmanual/03ssma.html

[74] "Microsoft asserts that because its headquarters are located within the Ninth Circuit, it must comply with Ninth Circuit precedent." U.S. v. Weaver, 636 F.Supp.2d 769 (U.S. District Court for the Southern District of Illinois 2009). See also: In Re Application of the United States of America for an Order Pursuant to 18 U.S.C. 2703(d) http://www.eff.org/cases/re-application-united-states-america-order

the law, and thus opened emails should not lose their protection under the law, regardless the location of the ISP or the requesting government agency.[75] 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.

When ISPs receive a subpoena or 2703(d) order from outside the 9th circuit, they can either comply with the order or refuse and go to court. Those 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.

Delivering To/From headers in response to subpoenas for email messages

Providers 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 181 days old that are provided to the government in response to a subpoena.

18 USC 2703(a) specifies that the government can use a subpoena or "d" order to obtain the contents of email communications that are older than 180 days.[76] However, non-content information[77] can only be

---

See also: "[A Ninth Circuit decision in Theofel et al. v Farey-Jones and Kwansy … held that opened emails on ISP servers are also in `electronic storage.' Therefore, as Microsoft receives and processes legal process for its online services in the Ninth Circuit, Microsoft discloses both opened and unopened emails in electronic storage for 181 days or less only pursuant to a search warrant." http://www.wired.com/images_blogs/threatlevel/2010/02/microsoft-online-services-global-criminal-compliance-handbook.pdf

[75] "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." 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 (2007) at 581.

"State and local law enforcement should also be aware that several large ISPs such as AOL,Yahoo, and Hotmail are currently providing e-mail content to law enforcement only pursuant to an ECPA warrant based on Theofel, supra, regardless of the location of the requesting governmental entity, service of the process, or maintenance of the records." http://www.ndaa.org/pdf/ecpa_isps_obtaining_email_05.pdf

[76] "a governmental entity may require the disclosure by a provider of electronic communications services of the **contents** of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days [with …] with prior notice from the governmental entity to the subscriber or customer if the governmental entity uses an …. **Subpoena** …. ; or obtains a [2703(d) order]."

[77] Other than customer record information specified in 18 USC 2703(c)(3).

obtained pursuant to a search warrant or "d" order.[78] Email headers have long been considered to be non-content (although this does not include the subject line),[79] which the 9th circuit confirmed in *United States v. Forrester*.[80]

As a result, Yahoo, Google and Microsoft have quietly established policies of scrubbing the "to" and "from" headers from email messages that are delivered to law enforcement agents in response to a subpoena.[81] In such instances, if government officials wish to compel the disclosure of those headers, they must go to the court and obtain a 2703(d) order. By taking this position, the ISPs have been able to force some degree of judicial review over a process that would otherwise bypass the courts.

---

[78] 18 USC 2703(c) specifies that "a governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (**not including the contents of communications**) only when the governmental entity obtains a warrant, … [a 2703(d) order or], has the consent of the subscriber or customer to such disclosure…"

A few specific categories of customer records can be obtained with a subpoena. 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),

[79] "Every Internet email message consists of a set of headers that contain addressing and routing information generated by the mail program, followed by the actual contents of the message authored by the sender. The addressing and routing information includes the email address of the sender and recipient, as well as information about when and where the message was sent on its way (roughly analogous to the postmark on a letter). See United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (email to/from addresses and IP addresses constitute addressing information)." Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Computer Crime and Intellectual Property Section, Criminal Division, DOJ (2009) http://www.justice.gov/criminal/cybercrime/ssmanual/ssmanual2009.pdf

[80] "[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." United States v. Forrester, 512 F.3d 500, 503 (9th Cir. Cal. 2008)

[81] 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 a senior member of the company's privacy team was alerted to the practices of its competitors by this author.

Multiple sources tell me that the Department of Justice is not happy about the interpretation of ECPA that these ISPs have adopted,[82] but it has not gone to court to compel the delivery of these headers pursuant to a subpoena. It is unclear if DOJ is worried about a negative ruling, or if it wishes to avoid any public discussion about the fact that ISPs are able to adopt such policies, fearing that other ISPs might do so if they knew they could.

It remains unclear why Google, Yahoo and Microsoft will not publicly confirm their interpretation of ECPA. However, there is likely a good reason why the companies that do not scrub the headers refuse to admit it: the possibility of civil liability for improperly disclosing non-content communications information.[83]

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

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.

18 USC 2702(b)(8) and 18 USC 2702(c)(4) similarly permit the disclosure of communications content and non-content:

> [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.

This language has been repeatedly watered down over the past decade,[84] often due to requests from telecommunications carriers who don't want to be put in the position of evaluating the degree of the

---

[82] When queried about the issue, Richard Downing, the assistant deputy chief of the Computer Crime and Intellectual Property Section at DOJ politely refused to comment (Email conversation with Richard Downing, Computer Crime and Intellectual Property Section, DOJ, January 28, 2010). I am still waiting for the results of a related FOIA request for information.

[83] "The ruling that the government seeks in this matter would force Yahoo! To either endure a contempt penalty in this court or become vulnerable to civil liability within the Ninth Circuit. This liability is by no means hypothetical – in Quon v. Arch Wireless, 529 F.3d 892 (9th Cir. 2008) cert. granted sub nom, City of Ontario v. Quon, 130 S.Ct.1011, cert denied sub nom, USA Mobility Wireless, Inc. v Quon, 130 S.Ct. 1011 (2009) the Court of Appeals for the Ninth Circuit held that an electronic communication service provider who turns over opened and stored text messages without a warrant or a viable exception is liable under the SCA as a matter of law." http://www.eff.org/files/filenode/inreusaorder18/yahooresponse.pdf at page 2, footnote 1.

18 USC §§ 2707, 2712; The government faces additional administrative discipline measures under § 2707(d).

[84] "Although the SCA has always permitted some voluntary disclosures, their scope has grown and changed since September 11th. Initially, the SCA only permitted voluntary disclosures when a provider inadvertently discovered a communication that appeared to relate to a crime.… the PATRIOT Act modified the SCA, allowing

emergency.[85] There is little case law on the emergency provisions, although in general, once a carrier receives a statement from the government certifying the emergency, it can disclose the customers' communications without the risk of liability.[86]

Because the law does not require ISPs to tell their customers when their private communications or non-content data associated with it has been 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 of them were requests for emergency assistance. Of these 25,000, just 300 were from the federal government.[87] The company

---

providers to voluntarily disclose content information to law enforcement if the provider reasonably believed that disclosure without delay was necessitated by `an emergency involving immediate danger of death or serious physical injury to any person.' Disclosure of non-content information was permitted in similar circumstances.

One year later, in November 2002, the Homeland Security Act expanded the emergency provision. With respect to content, it did so in three primary ways. First, it removed the requirement that there be immediate danger of injury or death. Second, it altered the requirement that the provider have a `reasonable' belief in danger, requiring only a `good faith' belief. Third, it allowed disclosure to any federal, state, or local governmental entity, not merely to law enforcement. The Homeland Security Act also added a requirement that the communications disclosed `relat[e] to the emergency.' In March 2006, Congress made a final set of changes, rendering the standards governing content and non-content effectively the same." Rosenbloom, Seth, Crying Wolf in the Digital Age: Voluntary Disclosure under the Stored Communications Act. Columbia Human Rights Law Review, Vol. 39, No. 2, 2008.

[85] "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.' Cyber Security Enhancement Act of 2002, H.R. Rep No. 107-497, at 12-13 (2002)." See: http://www.justice.gov/oig/special/s1001r.pdf, footnote 272 on page 261.

See also http://markey.house.gov/docs/telecomm/Verizon_wiretaping_response_101207.pdf at page 6.

See also: Statement by 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." http://www.wired.com/threatlevel/2007/03/att_verizon_we_/

[86] See, e.g., Jayne v. Sprint PCS, 2009 WL 426117 (E.D. Cal. 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).

[87] http://markey.house.gov/docs/telecomm/Verizon_wiretaping_response_101207.pdf at page 5.

has not released any statistics detailing how many of these 25,000 emergency requests it refused to comply with.

As the U.S. Internet Service Provider Association notes, "there is never an 'emergency' obligation on an ISP to disclose."[88] If a carrier says no, the government can always obtain a subpoena, "d" order, or search warrant, and compel the disclosure of 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.

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

For example, in June of 2009, an email message sent by Florida police officer to others in the law enforcement community showed up on the wikileaks.org website.[89] That email described his experiences interacting with several Internet providers and telecom carriers during a recent child exploitation investigation. When presented with the same details describing the emergency, MySpace, Yahoo and AT&T all had differing responses: MySpace immediately delivered the requested IP login information; Yahoo pushed back, but eventually delivered IP logs, but only those for logins that were more than 48 hours old; while AT&T refused to voluntarily provide any customer information in response to the police's request, and only delivered the requested records after the police obtained a subpoena compelling disclosure. [90]

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 like AT&T, in at least some situations, appear to have taken the position that they will not disclose information in emergencies. Other companies, like Verizon, have even argued in court that they have a 1st amendment right to disclose their customers' private information to 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, 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 for very limited circumstances. We require a subpoena when we need the financial information from the site, credit card info or sometimes IP information….

[88] U.S. Internet Serv. Provider Ass'n, Electronic Evidence Compliance: A Guide for Internet Service Providers, 18 Berkeley Tech L.J. 962 (2003).

[89] 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 it is valid. I have also attempted to get Yahoo! and AT&T to confirm the police officer's statements, but my contacts at the two companies were not willing to do so, on or off the record.

[90] Email on file with author.

> [I]f you are 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**."[91]

Because 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 this decision was simply a one off.

Charging the government for consumers' private data

Many telecommunications companies and Internet service providers seek and usually[92] receive payment from government agencies for the surveillance services that they provide, a practice that the law often permits.[93] 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

[91] http://lawmeme.research.yale.edu/modules.php?name=News&file=article&sid=925

[92] Just because a provider sends the government agency an invoice for surveillance services, doesn't 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 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." http://www.justice.gov/oig/reports/FBI/a0803/index.htm

[93] Providers are prohibited by 18 U.S.C. § 2706(c) from recovering the cost of producing phone records. It is also unclear if providers who insist on a Rule 41 order to deliver location information can seek compensation (A position several providers, such as Loopt have taken). See: Written Testimony of Al Gidari, ECPA Hearing, May 5, 2010 at page 6.

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."; Also: "Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance **shall be compensated therefor by the applicant for reasonable expenses** incurred in providing such facilities or assistance." 18 U.S.C. § 2518(4) (2006) (emphasis added); "[T]he Director of National Intelligence and Attorney General 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 ....The 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. §§ 1881a(h)(1)-(2). (emphasis added).

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 of not seeking compensation for surveillance and data disclosure 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.

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, I understand that at least MySpace, Facebook and Microsoft do not charge. MySpace's then-chef security officer confirmed that the company does not charge for the "thousands" of requests it receives from the government each year,[94] while well-informed sources confirmed similar policies at both Facebook and Microsoft.[95]

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.**"[96]

---

[94] Conversation with Hemanshu Nigam, at the OSTWG meeting, February 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 it has refused to respond to.

[95] Microsoft's law enforcement manual does not mention any policy of seeking compensation. See: http://www.wired.com/images_blogs/threatlevel/2010/02/microsoft-online-services-global-criminal-compliance-handbook.pdf. A well-informed source told me that the company does not charge for the information in 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 government assistance, although its law enforcement manual does say the company reserves the right to do so.

[96] http://judiciary.house.gov/hearings/pdf/Gidari100505.pdf

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 is the only telecommunications provider that lists its surveillance prices on a publicly accessible page on its website.[97] 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,[98] 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).[99] Likewise, Google's head of public policy revealed in comments at a public event 2009 that the company requests compensation for the assistance it provides to the government.[100] 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 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

---

[97] "To defer the cost to Cox of compliance, payment of the following minimum fees is required for all subpoena, court order and warrant requests . . . . Wiretap: **$3,500** for each 30 days — **$2,500** for each additional 30 days." Cox Communications, Notice to parties serving subpoenas on Cox Communications, http://www.cox.com/Policy/leainformation/default.asp. (last visited Oct. 29, 2009).

[98] 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. 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." Posting of Steven Aftergood to Secrecy News, Implementing Domestic Intelligence Surveillance ,http://www.fas.org/blog/secrecy/2007/10/implementing_domestic_intellig.html. (Oct. 15, 2007).

[99] "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]." Letter from Randal S. Milch, Senior Vice President, Legal & External Affairs & General Counsel, Verizon Business. to John D. Dingell, Chairman, U.S. H.R. Comm. on Energy & Commerce, to Edward J. Markey, Chairman, U.S. H.R. Subcomm. on Telecomm. & Internet, and to Bart Stupak, Chairman, U.S. H.R. Subcomm. on Oversight & Investigations 3–4 (Oct. 12, 2007), http://markey.house.gov/docs/telecomm/Verizon_wiretaping_response_101207.pdf page 10.

[100] "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." http://paranoia.dubfire.net/2009/06/shot-across-bow.html

US Marshals Office that were determined to be responsive to my request. When given the opportunity to object to the disclosure of its price list, Verizon argued that:

> "We 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). "[101]

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

> "[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."[102]

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 cryptome.org via a Digital Millennium Copyright Act notice.[103] On the same day, Facebook sent me an email, requesting that I remove a hyperlink from my personal Twitter account which linked to a copy of the company's law enforcement handbook that was hosted on the official website of the Wisconsin State Public Defender. Although I ignored their request, the file soon disappeared from the Wisconsin website, presumably after also being contacted by Facebook. [104]

[101] http://files.cloudprivacy.net/verizon-price-list-letter.PDF

[102] http://files.cloudprivacy.net/yahoo-price-list-letter.PDF

[103] See generally: 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 lead to significant media attention, both on the Internet and TV. See: http://www.wired.com/threatlevel/2009/12/yahoo-spy-prices/ and http://www.colbertnation.com/the-colbert-report-videos/258582/december-16-2009/the-word---spyvate-sector

[104] " Facebook Confidential Information on your Twitter Account," Email from Jeff Wu to Christopher Soghoian, December 2, 2010, on file with author.

PART III: Encouraging companies to compete on privacy

As the preceding two sections documented, 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, thus creating a market for privacy?

This section will first briefly explore the existing surveillance statistics that have been made public, both those pursuant to specific statutory requirements, as well as 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 the 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.

Government compiled aggregate surveillance statistics

Each year since 1997, the Administrative Office of the US Courts has compiled and published a detailed report on the number of law enforcement wiretaps and other electronic intercepts that occurred, at the state and federal level, in the previous year. The report is extraordinary in its high-quality[105] and detail, 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.

[105] "The AO has done an excellent job of preparing the wiretap reports." Statement by Senator Leahy, CONTINUED REPORTING OF INTERCEPTED WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS ACT -- (Senate - December 03, 1999), available at http://frwebgate.access.gpo.gov/cgi-bin/getpage.cgi?dbname=1999_record&page=S15228&position=all

Likewise, each year, the Department of Justice is required to submit several surveillance related reports to Congress. These include: A report regarding the use of pen registers and trap & trace devices by law enforcement agencies within the Department of Justice; [106] a report detailing the number of emergency disclosures of the contents of communications to the Department of Justice by Internet Service Providers, pursuant to USC 2702(b)(8);[107] and 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, "Section 215" requests for business records and tangible things for foreign intelligence purposes, and national security letters sent by the Federal Bureau of Investigation.[108]

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 DOJ similarly lack carrier information, although this is less of an immediate problem, since 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.

Company provided surveillance statistics

Over the past few years, a few service providers have voluntarily published statistics regarding the extent to which they receive government requests, and 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.[109] In 2007, in response to a query from several members of

[106] "The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice." 18 U.S.C. § 3126 (2009).

[107] "On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing … the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and a summary of the basis for disclosure in those instances where -- voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and the investigation pertaining to those disclosures was closed without the filing of criminal charges." 18 USC 2702(d).

[108] See sections 107 and 502 of the Foreign Intelligence Surveillance Act of 1978 (the "Act"), as amended, 50 U.S.C. § 1801 et seq., and section 118 of USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (2006).

[109] 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,

Congress, Verizon provided detailed information regarding the requests it had received from government agencies, which averaged 90,000 per year.[110] In 2009, a representative from Facebook told Newsweek that it was receiving between 10-20 requests from police per day.[111] Finally, in response to a copyright lawsuit in 2010, cable giant Time Warner revealed that it was receiving approximately 500 IP address lookup requests on average per month, nearly all of which come from law enforcement.[112] None of these companies have provided updated statistics since their initial disclosure.

In April 2010, Google announced its new Government Requests Tool, which reveals the number of government requests for user data the company received between July 1, 2009 and December 31, 2009, broken down by country. While the initial data set only covers a single six month period, Google pledged to update it twice per year going forward.[113] 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:

---

arguing that they are overly broad or that the litigants lack proper jurisdiction. About half of those rejected are resubmitted, on narrower grounds.

Hansel, *supra* note 102.

[110] http://markey.house.gov/docs/telecomm/Verizon_wiretaping_response_101207.pdf

In 2005, Verizon received 90,000 lawful requests and demands for customer information from federal, state and local officials, with approximately 36,000 coming from federal officials and 54,000 coming from state and local officials. In 2006, Verizon received 88,000 such requests and demands (approximately 34,000 from federal officials and 54,000 from state and local officials), and through September 2007, 61,00 such requests and demands (approximately 24,000 from federal officials and 37,000 from state and local officials). Verizon also received lawful requests for customer information from civil litigants numbering 57,000 in 2005, 69,000 in 2006, and 66,000 through September 2007.

Of the requests and demands coming from federal, state and local officials, requests for emergency assistance were approximately 23,700 in 2005 (240 of which were from federal officials), 25,000 in 2006 (300 of which were from federal officials), and 15,000 through September 2007 (180 of which were from federal officials)…

Verizon received in 2005 over 1,300 pen/trap court orders, as well as over 250 wiretap cort orders requested by federal and state law enforcement authorities. In 2006, we received over 800 pen/trap court orders and nearly 200 wiretap court orders. Through September 2007, these numbers are over 500 and 130, respectively. These numbers include instances in which wiretap or pen/trap orders were renewed.

[111] "[Facebook] says it tends to cooperate fully and, for the most part, users aren't aware of the 10 to 20 police requests the site gets each day." Nick Summers, *Walking the Cyberbeat*, NEWSWEEK, May 18, 2009, *available at* http://www.newsweek.com/id/195621.

[112] http://arstechnica.com/tech-policy/news/2010/05/time-warner-cable-tries-to-put-brakes-on-massive-piracy-case.ars

[113] "For this launch, we are using data from July-December, 2009, and we plan to update the data in 6-month increments." http://googleblog.blogspot.com/2010/04/greater-transparency-around-government.html

> 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. [114]

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. [115] 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.[116]

The current statistics are lacking

Both the currently released official surveillance government statistics, as well as the statistics voluntarily provided by 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.

---

[114] http://www.google.com/governmentrequests/overview.html

[115] "For its part, a Google spokesperson cut off a question about how many subpoenas it handles a year, saying `You know we don't discuss that.'" http://www.wired.com/threatlevel/2010/03/google-microsoft-ecpa

"As a matter of policy, we do not comment on the nature or substance of law enforcement requests to Google." Declan McCullagh, *How safe is instant messaging? A security and privacy survey*, CNET News, June 9, 2008, http://news.cnet.com/8301-13578_3-9962106-38.html (Google's response to the question "Have you ever received a subpoena, court order or other law enforcement request asking you to turn over information about a user's IM account?").

We do not comment on specific requests from the government. Microsoft is committed to protecting the privacy of our customers and complies with all applicable privacy laws. In particular, the Electronic Communications Privacy Act ("ECPA") protects customer records and the communications of customers of online services. As set forth above, however, Microsoft does not maintain records about our customers' use of the IM service and would have no information to provide in response to a request from law enforcement.

McCullagh, supra note 105 (Microsoft's response to the question "Have you ever received a subpoena, court order or other law enforcement request asking you to turn over information about a user's IM account?"). And "Given the sensitive nature of this area and the potential negative impact on the investigative capabilities of public safety agencies, Yahoo does not discuss the details of law enforcement compliance. Yahoo responds to law enforcement in compliance with all applicable laws." Id. (Yahoo's response to the question "Have you ever received a subpoena, court order or other law enforcement request asking you to perform a live interception or wiretap, meaning the contents of your users' communications would be instantly forwarded to law enforcement?")

[116] "We [Microsoft] would like to see more transparency across the industry … But no one company wants to stick its head up to talk about numbers." (http://www.wired.com/threatlevel/2010/03/google-microsoft-ecpa/)

For example, Verizon received 88,000 government requests in 2006, while Google received 3,000 requests from the US government during six months of 2009. 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 it complied with.
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.
5. The number of instances in which the company had nothing useful to deliver, due to data deletion policies, or the use of encryption in which it does not have the key.

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 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 their customers' data. The Federal government is not the only avenue for legislative action though – often, change starts with the states.[117]

[117] "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." New State Ice Co. v. Liebmann, 285 U.S. 262 (1932), Brandeis' Dissent.

For example, over the past several years, 46 states have adopted data breach statutes, all following California's lead in 2003. 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. Although letters describing the breach only went out to California residents, this had the effect of tipping off consumers, media, and other states' attorneys general. Soon enough, Choicepoint admitted that it had suffered a breach that impacted individuals from across the country.

States can play a significant role in shining a light upon companies' surveillance practices. Furthermore, Americans from all 50 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, California, given how many Internet service and application providers are based there):

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, detailing 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 shall disclose the relevant numbers for the state and the total for the country, en
4. Require that companies disclose the amount of money they charge the government for responding to requests for user data, if anything is charged at all, and the degree to which the company makes a profit from such disclosures.

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

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."[118]
>
> -- David Vladeck, Director of the FTC Bureau of Consumer Protection

The United States is unique among western countries, in that its primary privacy regulator, the Federal Trade Commission, is entirely focused on privacy violations by companies, but not the government. Contrast this to Europe and Canada, where their privacy commissioners are free to comment on matters of government surveillance. Thus, for example, in the same month, Canada's Privacy Commissioner condemned the proposed roll out of full-body scanners at airports[119] and launched an investigation into Facebook's privacy flaws.[120] 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 Department of Justice, 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 hook for the agency has been the privacy policies that both the Children's Online Privacy Protection Act (COPPA) and California law required companies to post on their websites. If a company claims to do something in its privacy policy, and it doesn't do so (or doesn't do it sufficiently), the FTC is in a position to act.

The most relevant of the FTC's privacy cases is the *Tower Records* settlement from 2004.[121] 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." When the company failed to protect end user's data from hackers, the FTC argued that Tower had failed to: "implement appropriate checks and controls on the

---

[118] Speech by David Vladeck, Director, FTC Bureau of Consumer Protection. http://www.ftc.gov/speeches/vladeck/091002nyu.pdf

[119] http://www.priv.gc.ca/media/nr-c/2010/op-ed_100107_e.cfm

[120] http://www.priv.gc.ca/media/nr-c/2010/nr-c_100127_e.cfm

[121] In the Matter of MTS, Inc., d/b/a Tower records/Books/Video (Agreement containing Consent Order, FTC File No. 032-3209, April 21, 2004), available at: www.ftc.gov/os/caselist/0323209/040421agree0323209.pdf.

process of writing and revising Web applications; adopt and implement policies and procedures regarding security tests for its Web applications; and provide appropriate training and oversight for their employees regarding Web application vulnerabilities and security testing."

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

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 to do so. What they should not be permitted to do though, is to proclaim their commitment to protecting their customers' privacy, and then actively subvert it by designing their systems to put 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.

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 simulative effect upon 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 so these consumers would then 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.

CONCLUSION

Although many companies claim to value and protect privacy, this article has clearly demonstrated 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 still continue to tout their commitment to protecting user data.

As a result of this lack of accurate information about companies' practices, there is simply no functioning market for this kind of privacy. Consumers have no way to evaluate each firms' practices, and as such, may in some cases entrust information to these firms that they might not otherwise have done 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. In this article, I outlined several ways to achieve this – the next step is to implement these policies.