Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era[†]

Christopher Soghoian[‡]

Work in progress, please do not cite.

Feedback is much appreciated. Send to csoghoian@gmail.com

[‡] Student Fellow, Berkman Center for Internet & Society, Harvard University. Ph.D. Candidate , School of Informatics, Indiana University. Email: csoghoian@gmail.com. Other research papers available at http://www.dubfire.net.

This paper was started while the author was a technology policy intern at the American Civil Liberties Union of Northern California, and was researched and completed while the author was a student fellow at the Berkman Center. The author has also been supported by a generous fellowship from the Institute for Humane Studies. Thanks to Aaron Brauer-Rieke, Benjamin Edelman, Albert Gidari, Nicole Ozer and Elizabeth Stollings for their feedback and assistance. The opinions expressed within, any mistakes and all omissions are of course my own.

Table of Contents

I. Introduction

Over the last few years, both consumers and corporate clients have rushed to move their data to "the cloud,"[1] adopting web-based applications and storage solutions provided by companies that include Google, Microsoft and Yahoo. Over 69% of Americans use webmail services, store data online, or otherwise use software programs such as word processing applications whose functionality is in the cloud.[2] This trend is only going to continue.

The shift to cloud computing exposes end-users to privacy invasion and fraud by hackers. Cloud computing also leaves users vulnerable to significant invasions of privacy by the government, resulting in the evisceration of traditional Fourth Amendment protections of a person's private files and documents. These very real risks associated with the cloud computing model are not communicated to consumers, who are thus unable to make an informed decision when evaluating cloud based services.

This paper will argue that the increased risk that users face from hackers is primarily a result of cost-motivated design decisions on the part of the cloud providers, who have repeatedly opted to forgo strong security solutions. These vulnerabilities can easily be addressed through the adoption of industry standard encryption technologies, which are already in widespread use by online banks and retailers. Cloud providers must enable these encryption technologies, and more importantly, turn them on by default. This paper will argue that the failure of cloud computing companies to provide these technologies is a strong indicator of a market failure. Fixing this market failure may require user education in order to stimulate demand for safer solutions, or even the threat of government regulation.

As for the even more troubling intrusion upon user privacy performed by government agencies, fault for this privacy harm does not lie with the service providers; but the inherently coercive powers the government can flex at will. The third party doctrine, which permits government agents to obtain users' private files from service providers with a mere subpoena, is typically the focus of privacy scholars. However, this paper will argue that this doctrine becomes moot once encryption is in use and companies no longer have access to their customers' private data. The real threat to privacy lies with the fact that corporations can and have repeatedly been be forced to modify their own products in ways that harm end user privacy, such as by circumventing encryption.

Cloud computing providers are in an unenviable situation – since there is little they can do to guarantee their customers protection from the government's watchful gaze. While on one hand, public interest groups and activists will criticize these companies for failing to protect their customers' privacy,[3] and on the other, the government can quietly force them to circumvent any privacy enhancing technologies that they do deploy.

This paper is organized as follows. Part I introduces the concepts behind cloud computing, and the technical shifts that have made it possible for many users to unknowingly switch to cloud solutions. Part II will explore privacy and security related threats which users face from hackers, and the failure of service providers to protect users from

---

[1] "Cloud Computing Services" involve "a software and server framework (usually based on virtualization)" that uses "many servers for a single software-as-a-service style application or to host many such applications on a few servers." See: "Perspectives on Cloud Computing and Standards," NIST, Information Technology Laboratory, http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloud-computing-standards_ISPAB-Dec2008_P-Mell.pdf (last visited Mar. 11, 2009).

[2] "Cloud Computing Gains in Currency," Internet and American Life Project, (Sep. 12, 2008), *available at* http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency.

[3] See generally, Complaint and Request for Injunction, Request for Investigation and for Other Relief, In the Matter of Google, Inc. and Cloud Computing Services, http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf

them. Part III focuses on the trickier issue of intrusions by the government, and the ultimate inability of service providers to protect their users from these threats. Part IV concludes with policy recommendations, both legal and technical.

I. Cloud computing

One of the defining characteristics of the personal computing paradigm is that users maintain physical control over their files and data. In fact, it was the departure from the mainframe computing model, in which users merely operated on slices of a central server's time and resources that marked the beginning of the personal computing era.

Personal computing users are able to make use of word processing programs such as Microsoft's Word in order to write memos, reports and letters. Likewise, consumers and businesses can turn to Microsoft's Excel and Intuit's Quicken in order to manage their finances and balance their books. Finally, home-photography buffs can use Apple's iPhoto, Adobe's Photoshop and other programs to organize, edit and catalog their digital photo collections.

This computing model has become firmly ingrained in the consciousness of consumers, and as such, we have become used to our documents, music, and photographs residing on our own personal devices as well as relying on our own computing resources to process and display our data. If we run out of storage space, or a task takes far too long, the solution is to upgrade our own computer – and likewise, if our computer suffers a hardware failure, is lost or stolen, we often lose our files.

In recent years, the computing industry has turned away from this personal computing model, and shifted towards online services, commonly described as “software as a service” or “cloud computing.” This paradigm, in which the user's web-browser acts as a “thin client” and remote servers perform the majority of the data processing is rapidly being adopted by both consumers and businesses. As such, this model already plays a key role in the United States economy.[4]

The first application to move to the cloud was electronic mail – perhaps due to the fact that the use of the service already required Internet access. However, in time, other applications soon moved online. Google's Apps suite is the market leader in this area,[5] providing word processing, spreadsheets and presentation software functionality via a web browser. Microsoft, Adobe and Intuit have been quick to follow, by releasing Web-based versions of their Office,[6] Photoshop[7] and Quicken products.[8]

Cloud computing allows a whole collection of resources such as applications, storage space and processing power to be delivered over the Internet. Hundreds of thousands of computers, located in data centers around the world handle the processing and storage of data for millions of individual users. The cloud computing model is deemed by many commentators to be the future of computing.

---

[4] A March 2009 study expects corporate IT spending on cloud services to grow almost threefold, reaching US$42 billion, by 2012. See: http://www.informationweek.com/blog/main/archives/2008/10/idc_says_it_clo.html

[5] “This shows that Google's word processing and spreadsheet products have a noticeable lead over what may be its nearest rival, Zoho.” See: http://www.readwriteweb.com/archives/google_docs_web_office_leader.php

[6] See generally, Office Live, http://www.officelive.com/

[7] See generally Photoshop Express, https://www.photoshop.com/express/landing.html

[8] See generally, Quicken Online, http://quicken.intuit.com/

Many firms wishing to draw attention to their own products have adopted and borrowed terms associated with "cloud computing," such as "Web 2.0", "software as a service" and other in-fashion buzzwords. As a result, there is little agreement on the actual definition of "cloud computing."[9] For the purpose of this paper, the term "cloud computing" will be used to apply to software offerings where the application is executed in a web browser, via software code that is downloaded (as needed) from a remote server that also stores users' files.[10]

A. Benefits of cloud computing for service providers

The cloud computing model brings a lot of benefits to service providers: Reduced piracy, the ease of denying access to troublesome users, protection of sensitive technology, and the ability to serve carefully targeted advertising to customers.

The problem of unauthorized copying is almost non-existent when software is delivered via the web – something that computer game industry has also been quick to learn.[11] This is because much of the computation occurs on the software provider's own servers. Since this code is never provided to the user, it cannot be copied.

Another benefit to cloud computing is the ability to easily terminate access to particular users. Software providers are able to maintain control over access to their services, often via a unique account and password per customer. If a company wishes to cut off access to a particular customer, this can be done by simply suspending an individual account.

Furthermore, cloud computing makes it far easier to protect trade secrets. For example, companies like Adobe whose flagship Photoshop product contains proprietary image-altering algorithms may wish to keep such technology secret from their competition. Whereas previously, a competitor could purchase a copy of Photoshop, run it on a desktop computer, and reverse engineer the product's key algorithms.[12] Under the cloud computing paradigm, the user's Web browser submits an image to Adobe's servers, which apply the algorithm, and then return the modified image. Since the secret algorithm is never executed on the user's computer, reverse engineering is made exceedingly difficult.

Cloud services also allow software vendors to easily embed advertisements into their offerings, and to use sophisticated data mining algorithms to display advertisements related to the vast amounts of private data that users upload.

Finally, cloud computing providers can be certain that end users are always running the most up-to-date version of their software, a problem that has plagued the traditional PC industry. Cloud vendors can apply the fix to their own

---

[9] "While almost everybody in the tech industry seems to have a cloud-themed project, few agree on the term's definition." See: The Internet Industry Is on a Cloud -- Whatever That May Mean, http://online.wsj.com/article/SB123802623665542725.html

[10] While pure remote storage or computing services such as Amazon's S3 are commonly described as cloud services, they are beyond the scope of this paper.

[11] FIXME

[12] Reverse Engineering is generally defined as the process of "starting with the known product and working backward to divine the process which aided in its development or manufacture." See: *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974). See also: The Law and Economics of Reverse Engineering, Pam Samuelson, http://www.yalelawjournal.org/pdf/111-7/SamuelsonFINAL.pdf

servers, without requiring that users choose to update it themselves. This ability to roll out instant updates across an entire product line reduces tech support costs, and helps to protect the company's reputation from being damaged by claims of shoddy workmanship or poor security practices.

B. Benefits of cloud computing for end-users

For the consumers and businesses that have switched to cloud based services, there are a number of benefits including price, reliability, accessibility as well as the ease of access independent of a specific computer.

Most cloud computing services are either free or significantly cheaper than more traditional desktop offerings.[13] Consumer orientated services are generally "free," in so far as users do not pay money for access, but instead submit to behavioral advertising and data mining of their activities.[14] Commercial editions of cloud services often come with a direct financial cost, but one which is far less than comparable desktop software. Of course, Microsoft Office and Google Docs are not equal in features, but Google's product suite is often *good enough* for school work, as well as the simple word processing and spreadsheet tasks performed by many employees.[15]

Many of the cloud based services include built-in revision control systems,[16] which enable a user to immediately access past versions of a document. Files are automatically backed up, at regular intervals, and stored on multiple servers around the country. As a result, hardware failure in the user's computer will not result in the loss of any data. Furthermore, in the event that the user suffers a hardware failure, they merely need to open a web-browser on a different computer, and can then continue editing their documents where they had previously left off.

Since the applications and user's files are stored online, they are accessible from anywhere in the world. A user can sit down at a new computer (even miles from their home) and instantly access a copy of her documents. Furthermore, since most of the heavy duty processing is performed on the remote servers and not on the user's computer, cloud computing extends the usable life of older computer hardware as well as providing data access to lower powered devices such as mobile phones.

C. Cloud creep and the rise of cloud services as the pre-installed default

While some users may choose to switch to cloud based services, others are not as fortunate and often this decision is made without their knowledge.

---

[13] For example, Google charges $50 per year per employee to businesses that use its Apps Premier Edition service. See: http://www.google.com/apps/intl/en/business/editions.html

This is significantly less than the $122 that businesses are estimated to spend per employee for just email service. See: http://www.gartner.com/DisplayDocument?doc_cd=146730&ref=g_rss

[14] See generally, "STOP THE ABUSE OF GMAIL", http://www.law.duke.edu/journals/dltr/articles/pdf/2005dltr0014.pdf

[15] http://blogs.pcworld.com/techlog/archives/003783.html

[16] "Revision control …. is the management of changes to documents, programs, and other information stored as computer files." See: http://en.wikipedia.org/wiki/Revision_control

Due to the significant reductions in licensing and support costs, many corporate and government IT managers are making the switch. Compared to the $500 list price for the full version of Microsoft Office Professional 2007, Google's $50-per-year price tag is a bargain – especially given that it includes telephone, e-mail and web support. Corporate enterprise managers are able to re-brand the Google Apps products with their own companies' logos. The services also plug directly into existing IT infrastructure. For example, corporate Google Mail customers can configure the service to use their own Internet domain names, making the switch oblivious to outsiders and customers who might otherwise recognize the telltale 'gmail.com' email addresses.

As a result, incoming students at many universities are now issued Google accounts, through which they can access the company's products to compose email and write term papers.[17] University students are not alone in this switch – before he was tapped to become the Federal Chief Information Officer, Vivek Kundra switched 38,000 Washington DC employees from Microsoft Office to Google Docs.[18]

While some students and employees realize that they are using cloud based services, many others may not, particularly when the services have been rebranded and stripped of Google's logos.

At the consumer level, cloud services are also making inroads through the use of pre-installed desktop icons on new PCs, particularly in low end devices. Over the past year, sub $400 "netbook" portable computers have taken the computing industry by storm. The manufacturers of these devices operate with extremely low profit margins, which they hope to make up in volume.[19] As a result, the netbook makers are trying many possible ways to lower their own costs. One of the main ways they have done this to abandon Microsoft's operating system and Office suite. In addition to pre-installing these computers with the Linux operating system, several manufacturers also ship their netbook products with prominent icons for Google's Docs and Spreadsheets tools.

In addition to the general industry trends that are pushing many towards cloud based services, new technologies make such transitions less obvious to end-users. Two of these are now highlighted: single site browsers, and offline content.

D. Single site browsers

The shift to cloud computing moved much of a user's normal activity to the Web browser. While this certainly lowers many barriers to user adoption, such as negating the need to download and install specific applications, this transition also raises a number of security and usability issues. For example, Web browsers generally store all of a user's saved passwords, browsing history and other sensitive information in a single place. As such it is possible for malicious websites to exploit browser vulnerabilities in order to steal information associated with other existing or

---

[17] "In an effort to save money and increase technological opportunities for students, University of Minnesota colleges will allow students and staff to switch their Internet messaging services to Gmail and other Google Apps …. The school eventually plans to make the use of Google Apps mandatory for all students and faculty as a more cost-efficient method of operating." See: http://badgerherald.com/news/2009/05/01/u_of_m_to_go_with_gm.php

[18] "Last year, Vivek switched 38,000 D.C. employees to Google Apps from Microsoft Office …. The nation's new CIO apparently is a big Google Apps fan, enthusiasm that generated all kinds of open-source punditry last week. " See: http://www.microsoft-watch.com/content/corporate/one_nation_under_google.html

[19] Over 14 million netbooks were sold in 2008, with projected sales of 30 million devices in 2009. http://arstechnica.com/hardware/news/2009/01/asus-acer-strong-netbook-sales-in-09-is-30m-possible.ars

previous browsing sessions – such as a logged in email account or online banking session.[20] It is for this reason that some security experts recommend that consumers use one web browser for general surfing, and another for more sensitive tasks, such as online banking.[21]

Seeking to mitigate these risks, Web browser vendors have released single site browser technology, the most advanced of which is Mozilla's Prism tool for its Firefox platform.[22] Prism and the other single site browsers allow a user to "split web applications out of the browser and run them directly on the desktop."[23] A Prism user can create a dedicated icon on their desktop for any Web site they regularly visit. When that icon is clicked, a dedicated browser window will open taking them to the pre-assigned Web site. Each Prism instance maintains its own profile for browser preferences and user data, and each Prism application also runs as its own system process. The end result is that a malicious website accessed from one Prism session (or a Firefox browser window) is unable to access any of the private data associated with another Prism application.

In addition to these security benefits, Prism brings several changes to the user interface. By default, Prism applications do not show any of the browser's traditional branding. The web site address of the current page is not displayed, there are no forward, back or refresh buttons, nor is there any way to see when the user is or isn't connecting via a secure, encrypted connection.[24]

While PC manufacturers and corporate IT managers are already installing links to cloud based services on user's desktops, Prism and other Single Site Browser technologies make this process even easier. Particularly for end-users as yet unfamiliar with Web-based word processing and office tools, Prism can make these sites seem like regular applications, and make it possible to ignore the fact that the services are Internet based at all.

E. Offline content

---

[20] "[A]ttackers could compromise a Gmail account--using a cross-site scripting vulnerability--if the victim is logged in and clicks on a malicious link." See: http://news.cnet.com/Gmail-cookie-vulnerability-exposes-users-privacy/2100-1002_3-6210353.html

"Security researcher Petko Petkov has revealed a cross-site request forgery vulnerability in Gmail that makes it possible for a malicious web site to surreptitiously add a filter to a user's Gmail account that forwards e-mail to a third-party address." See: http://arstechnica.com/software/news/2007/09/cross-site-request-forgery-vulnerability-found-in-gmail.ars

"Researchers from Princeton University today revealed their discovery of four major Websites susceptible to the silent-but-deadly cross-site request forgery (CSRF) attack -- including one on INGDirect.com's site that would let an attacker transfer money out of a victim's bank account …. The CSRF bug they found on ING's site would have let an attacker move funds from the victim's account to another account the attacker opened in the user's name, unbeknownst to the user. Even using an SSL session wouldn't protect the user from such an attack" See: http://www.darkreading.com/security/app-security/showArticle.jhtml?articleID=211201247

[21] See generally: http://securosis.ehclients.com/blog/making-the-move-to-multiple-browsers

[22] See generally, Mozilla Prism: http://labs.mozilla.com/projects/prism/, See also Fluid for Safari: http://fluidapp.com/

[23] See: http://labs.mozilla.com/2007/10/prism/

[24] "Personal computing is currently in a state of transition. While traditionally users have interacted mostly with desktop applications, more and more of them are using web applications. But the latter often fit awkwardly into the document-centric interface of web browsers. And they are surrounded with controls–like back and forward buttons and a location bar–that have nothing to do with interacting with the application itself." See: Introducing Prism, http://labs.mozilla.com/2007/10/prism/

As applications first started to move into the cloud, one of the few obvious disadvantages was that users had to be connected to the Internet in order to access their documents and personal files. When on an airplane, or in a public place without wireless Internet access, users found themselves unable to access files that would have otherwise been just a few clicks away.

Google was the first major provider to try and address this issue, releasing its Gears browser add-on in 2007.[25] This software tool provided a standard application programming interface (API) which websites could use to enable offline data storage and access. Google initially only enhanced its "Reader" product with Gears functionality. The company later added support for its Docs, Spreadsheets and Gmail products.[26] Thus, with Gears installed, a Gmail user can have almost complete access to their inbox and draft new emails when away from an Internet connection. Once a connection is re-established, the browser will automatically synchronize with Google's servers, sending the stored messages and downloading those newly received.

SWhile Google's Gears was the first offline API to be released, other companies such as Microsoft and Adobe have since released their own software tools. In 2008, offline support was added to the specification for the HTML5 standard. As a result, the latest versions of Firefox and Apple's Safari already include support for this technology,[27] without the need for the user to download install any additional software.

F. Confusion

The mass deployment of cloud based services, particularly when coupled with single site browser and offline content technology will likely lead to a significant risk of confusion for end users. As computer manufacturers, employers and universities deploy cloud based tools on the desktop, many users may fail to realize that they are in fact using an Internet based service. This risk of confusion will be increased when those same cloud based applications lack any recognizable browser branding and continue to function when the user is not connected to the Internet.

In the not too distant future, a non-expert user will sit down at a new computer (perhaps provided to them by an employer or purchased at a store), click on the "Word Processor" link on the computer's desktop, and will be able to begin typing a document. The application will appear similar to other word processors, previously used, but will actually be a sophisticated Web application running in a cloaked Web browser. This shift to a Web based technology will be accompanied by a radical shift in the user's rights and "expectation of privacy," at least as recognized by the courts; even if the user herself does not recognize that her documents are ever leaving her computer. Many users will be completely unaware that this shift has occurred, at least until it is too late.

---

[25] "Google Launches Gears Open Source Project to Bring Offline Capabilities to Web Applications", http://www.google.com/intl/en/press/pressrel/gears_20070530.html

[26] See: "Google Docs pulls head out of the cloud, goes offline", http://arstechnica.com/old/content/2008/03/google-docs-pulls-head-out-of-the-cloud-goes-offline.ars and "Gmail finally gets offline access—with caveats", http://arstechnica.com/web/news/2009/01/gmail-finally-gets-offline-accesswith-caveats.ars

[27] See: http://webkit.org/blog/126/webkit-does-html5-client-side-database-storage/

https://developer.mozilla.org/en/Offline_resources_in_Firefox

http://www.internetnews.com/xSP/article.php/3672011

II. Many cloud computing services are vulnerable to hackers

The vast majority of cloud computing services are, by default, insecure. Often, usernames and passwords are transmitted to remote servers via unencrypted network connections. In cases where encryption is used, it is typically only used to transmit the initial login information, while all subsequent data is sent *in the clear*.[28] This data can easily be snooped by hackers. This puts users at a significant risk when they connect to the services over a public wireless network.[29] These flaws are rarely if ever disclosed to end-users, who are then placed at risk.[30] As an example, consider the following two scenarios:

Alice, a student, decides to do her homework at a coffee shop, using her laptop and a copy of Microsoft Word. In such a situation, it will be exceedingly difficult for a malicious person (perhaps sitting at another table or across the street) to breach her privacy. If the evil-doer is sitting behind her, he could perhaps read over Alice's shoulder, but such activity would soon become obvious. If he is extremely tech savvy, perhaps he can hack into Alice's computer – but this will require that Alice's operating system have an un-patched flaw, and will further require that the adversary perform the *active* task of breaking into Alice computer in order to steal a copy of her documents.

Compare this to a similar situation, in which Alice is using Google Docs on her laptop, at the same coffee shop. In this case, every character that Alice types into her word processing document is transmitted to Google's remote servers over the unsecured wireless network.[31] Due to the fact that Google's services do not, by default, use encryption to transmit user data, the attacker can use one of many off-the-shelf tools to *passively* "sniff" the network and capture Alice's private data as it is transmitted to the company's servers. Worse, the hacker can capture the credentials necessary to later impersonate Alice, thus enabling him to later connect to her account and browse through older documents and emails.

Off the shelf tools have been written to automate these widely publicized vulnerabilities in many cloud computing services.[32] While the service providers have known about these flaws (and the ease with which they can be

---

[28] "'In the clear' is a term of art which means without encryption." See: Paul Ohm, Good Enough Privacy, 2008 University of Chicago Legal Forum 1. (citing Neil Daswani, Christoph Kern, and Anita Kesavan, Foundations of Security: What Every Programmer Needs to Know 204 (Apress 2007)).

"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." http://www2.seattle.intel-research.net/~jjung/FormativeUserStudy4CHI.pdf

[29] "[T]he broadcast nature of Wi-Fi means that anyone within range of the network can receive and potentially read transmissions intended for any other device on the network." http://www2.seattle.intel-research.net/~jjung/FormativeUserStudy4CHI.pdf

[30] Despite living in a technologically sophisticated area of the U.S., the participants were not aware that information sent over Wi-Fi could be seen by others." http://www2.seattle.intel-research.net/~jjung/FormativeUserStudy4CHI.pdf

[31] In some cases, this happens in real-time, in order for features like spell-check to work. In others, documents will be automatically saved to a remote server at regular intervals.

[32] http://fscked.org/blog/fully-automated-active-https-cookie-hijacking

exploited) for several years, the service providers continue to ship products with unsafe default settings,[33] and in some cases, not offer any protection to end users.[34]

Over the years, Microsoft has often received criticism for the poor security of its products, which left users vulnerable to viruses and other forms of malicious software. The vast majority of this criticism was due to the fact that many companies and home users had not applied security patches, and were thus running vulnerable code. The company made significant progress in improving end user security, primarily by making it easier for users to automatically stay up to date with software updates. Yes, flaws are still discovered and publicized in Microsoft's products – but the company usually fixes these within a matter of weeks, and then provides free updates to its customers.[35] Except during the short period between when a new vulnerability is disclosed, and when a patch is released and then installed, Microsoft's customers are for the most part secure. At the very least, a Windows user can edit a document on their own computer with the confidence that no one else can read what is being written.

Users of cloud computing services lack the basic security which users of traditional PC based software may take for granted. Google, the market leader, and nearly all other leading cloud providers offer products that are by default vulnerable to snooping, account hijacking, and data theft by third parties.[36] Every time a user logs into their Google Mail, Docs, Flickr, Facebook or MySpace account from a coffee shop or other public wireless network, they risk having their private data stolen by hackers.

This problem is not due to the Web based nature of these services. Consumers are able to safely check their online bank accounts, order books from Amazon, or trade stocks with an online broker while using open wireless networks without any risk of account hijacking or data theft. Yet this private and valuable information flows over the same Internet connection that Google, Facebook and MySpace have somehow been unable to secure.

A. The benefits of network encryption

Bank of America, American Express and Amazon[37] all use the industry standard SSL encryption protocol to insure that all customer information is securely transmitted over the network.[38] This technology enables a user to safely conduct

---

[33] "Default settings are pre-selected options chosen by the manufacturer or the software developer. The software adopts these default settings unless the user affirmatively chooses an alternative option." See: Kesan, Jay P. and Shah, Rajiv C., Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics. Notre Dame Law Review, Vol. 82, pp. 583-634, 2006

[34] "Hotmail, Yahoo Mail, and Facebook … remain vulnerable to a so-called "man-in-the-middle attack" in which someone on the same Wi-Fi network hijacks the session cookies that are transmitted between a user's browser and a Web site." See: http://news.cnet.com/8301-1009_3-10023958-83.html

[35] Microsoft also provides free updates to users who are running unauthorized ("pirated") copies of its software. The rationale for this is that the Internet benefits when these users have patched their computers, as this makes it much more difficult for viruses and other malicious software to spread (which might otherwise infect Microsoft's legitimate customers).

[36] Adobe's Photoshop Express is a rare exception to the norm. This service is only available via a secure SSL encrypted session.

[37] While Amazon uses encryption to protect communications related to payment, it does not protect purchase history and recommendations. See: http://news.cnet.com/8301-1009_3-10023958-83.html

[38] In fact, it is impossible to connect to the web sites of both Bank of America and American Express using anything *but* an encrypted session. For example, typing http://www.americanexpress.com automatically redirects the user's browser to https://www.americanexpress.com.

business online, without the risk of a hacker capturing her private data as it crosses the network. This is because to third parties, her encrypted communications appear as undecipherable gibberish.

Most cloud based services transmit nearly every single bit of a user's data to the service's central servers over the network in the clear. In some cases, this even includes the username and password used to login to the user's account, significantly raising the risk of account theft.[39] This information can be captured with an off the shelf tool known as a "packet sniffer." Some operating systems, such as Linux and Apple's Mac OS even include these data capture tools out of the box.[40]

While most cloud services do not offer any encryption at all, Google does at least offer SSL encryption to the users of its services. However, it does so as an unadvertised option, which is disabled by default.[41] Other cloud providers such as Yahoo and Facebook do not offer SSL protection for their customer's communications. Even if a customer of these services wishes to protect herself from third party snoopers, there is nothing that she can do. Of course, Facebook, Yahoo and Microsoft *could* offer SSL. Likewise, they and Google could even turn it on by default, so that all customers were automatically protected from data sniffing attacks.

Contrast this to the security of online banks – users don't have to go out of their way to login to the "secure" front-end to their bank's website. They don't have to manually enter a different URL, or select a hidden configuration option. Consumers simply go to the bank's website, and login. Everything else is taken care of for them.

B. Why do cloud providers opt to leave users exposed?

---

[39] For example, MySpace users send their usernames and passwords to the site over an unencrypted connection.

[40] Both Mac OS and most Linux distributions include tcpdump. This tool is not particularly easy to use, and so many users opt for the far more user friendly 'Wireshark.'

[41] Customers of Google's services can enable security on a case-by-case basis by connecting to a different URL for the various Google services. That is, rather than connecting to http://mail.google.com, users must connect to https://mail.google.com. Due to the fact that web browsers default to http (if nothing else is specified), a user who simply types "mail.google.com" into her web browser will be sent to Google's insecure servers.

In 2008, more than a year after Google was first notified about attackers in which its customers account authentication tokens could be hijacked, the company released a new feature to enable automatic encryption. See: http://gmailblog.blogspot.com/2008/07/making-security-easier.html

The company's help page for the SSL-by-default features notes that "If you sign in to Gmail via a non-secure Internet connection, like a public wireless or non-encrypted network, your Google account may be more vulnerable to hijacking. Non-secure networks make it easier for someone to impersonate you and gain full access to your Google account, including any sensitive data it may contain like bank statements or online log-in credentials. We recommend selecting the 'Always use https' option in Gmail any time your network may be non-secure." See: http://mail.google.com/support/bin/answer.py?hl=en&ctx=mail&answer=74765

Other than a single blog post in 2008 noting the new feature and an item in the company's help website describing the feature and the risks it protects against, the company has done nothing to warn users of the very real risks that they face if they do not enable this option. Users who never explore their configuration options and stumble upon the SSL setting are unlikely to learn of the risks or enable the protection feature.

Secure Socket Layer (SSL) is a technical standard which is supported by every modern web browser and every popular web server.[42] The free open-source Apache web-server, which powers most popular websites,[43] includes SSL support by default.[44]

Defending the company's decision to not enable SSL encryption by default, a Google spokesperson stated that:

> "We use [SSL encryption] to protect your password every time you log into Gmail, but we don't use [SSL encryption] once you're in your mail unless you ask for it …. Why not? Because the downside is that [SSL encryption] can make your mail slower. Your computer has to do extra work to decrypt all that data, and encrypted data doesn't travel across the internet as efficiently as unencrypted data. That's why we leave the choice up to you."[45]

This "choice" is a false one, given that Google's customers do not receive notice of the risks they face if they do not seek out this unadvertised option.[46] However, the company does take the time to advertise the security of its products as a key feature.[47] Furthermore, Google does not offer customers this same "choice" when using its Google Health product, which allows consumers to access their health records online. That product is only available over an SSL encrypted connection, likely due to the Health Insurance Portability and Accountability Act.[48]

Even if companies genuinely wish to offer their users a choice over the ability to enable or disable encryption, the default option is critical, since so few people will ever modify it.[49] Furthermore, while the importance of safe defaults

---

[42] SSL was designed by Netscape and first released in 1995. This was the basis for an IETF standardized protocol, known as Transport Layer Security (TLS). SSL had numerous security flaws, and so modern web browsers all use TLS to encrypt their communications. However, the encryption of Web traffic is still commonly referred using the name of the TLS predecessor: SSL. See: The Transport Layer Security (TLS) Protocol Version 1.2, http://tools.ietf.org/html/rfc5246

[43] Apache is used by more than 50% of the servers on the web. See: http://news.netcraft.com/archives/2009/01/16/january_2009_web_server_survey.html

[44] In fact, Ben Laurie, one of the primary developers for Apache/SSL works for Google.

[45] See: http://gmailblog.blogspot.com/2008/07/making-security-easier.html

[46] There is no mention of the SSL encryption option on the main login page for any of Google's services.

[47] The homepage for Google Docs states "Files are stored **securely** online" (emphasis in the original) and the accompanying video provides further assurances of the security of the Google Cloud Computing Service. See: "Welcome to Google Docs," https://docs.google.com/.

Google also explicitly assures consumers that "Google Docs saves to a secure, online storage facility . . . without the need to save to your local hard drive." See: "Getting to know Google Docs: Saving your docs," http://docs.google.com/support/bin/answer.py?answer=44665&topic=15119

[48] See: http://www.google.com/health which automatically redirects to https://www.google.com/health

[49] "Default options have an enormous impact on household 'choices.' Such effects are documented in the literature on 401(k) plans. Defaults affect 401(k) participation, savings rates, rollovers, and asset allocation. For example, when employees are automatically enrolled in their 401(k) plan, only a tiny fraction opt out, producing nearly 100% enrollment. But when employees are not automatically enrolled, less than half enroll on their own during their first year of employment." See: Optimal Defaults, James J. Choi, David Laibson, Brigitte C. Madrian and Andrew Metrick, The American Economic Review, Vol. 93, No. 2, Papers and Proceedings of the One Hundred Fifteenth Annual Meeting of the American Economic Association, Washington, DC, January 3-5, 2003 (May, 2003), pp. 180-185

has been widely documented by scholars in the fields of computer science, economics and law, many companies still opt for unsafe defaults, and instead blame users for not seeking out and enabling those options.[50]

A far more likely reason why Google has not offered SSL by default and other companies have opted to forgo SSL completely is the issue of cost. Simply put, providing an SSL encrypted connection takes significantly more processing power and memory for a Web server to provide than a "normal" unencrypted connection. For example, if a common Web server can normally process 30,000 simultaneous connections, it might only be able to handle 5,000 simultaneous SSL encrypted connections.[51] Thus, enabling SSL by default will significantly increase the cost of providing services to end-users, simply due to the massive increase in the number of servers required to handle and process all of those encrypted connections.

Banks and online merchants are legally required to bear the financial burden of online fraud, with consumer liability typically capped at just $50.[52] This responsibility provides the banks and merchants with a strong incentive to encrypt their customers' data as it is transmitted over the Internet. Doing so will significantly reduce the risk of fraud or data loss, for which they must otherwise pay.[53]

Unfortunately, similar incentives do not exist for the cloud computing providers. Most of these services do not charge their customers anything for the services that they provide, and thus never handle sensitive financial information. While many customers might feel that the information which they have entrusted to Google and Yahoo is sensitive, this data often does not fall into one of the select categories for which legally required data security standards exist, such as for medical data, social security numbers, and financial information.

While most users' word processing documents or photo collections may not be that valuable to a fraudster, an email account can have considerable value – due to the fact that inboxes routinely contain passwords and account information for other websites. For example, many Web sites will resend a password to a user's email address in the event that the user forgets her password. Thus, a poorly secured email account can be leveraged to gain access to a victim's bank account, brokerage account or online health records.

"A Pew Internet & American Life Project study from August 2000 found that 84% of Internet users in the United States were concerned about businesses and strangers getting their personal data online. However, 56% did not know about cookies. More notably, 10% said they took steps to block cookies from their PCs. However, a study by Web Side Story found the cookie rejection rate was less than 1%. These data show that while people were concerned about their online privacy, they were unaware of the most significant technology that affects online privacy. While a small proportion of these people claimed to have changed the default setting, the data actually show that a very small percentage, less than 1%, actually change the default setting. In sum, despite the overwhelming concern for privacy, almost everyone deferred to the default setting and accepted cookies." See: Kesan, Jay P. and Shah, Rajiv C., Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics. Notre Dame Law Review, Vol. 82, pp. 583-634, 2006.

[50] "Facebook appears to have a strategy of dumping all the really hard security decisions on the users -- so that they can respond to criticism by blaming users for not turning off features X and Y. Searchability by default may be in their short-term financial interest, but the end result can too easily be unusable security plus unsafe defaults." See: Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed, page 742.

[51] These numbers are just examples, and are not the result of testing.

[52] http://www.fdic.gov/regulations/laws/rules/6500-1350.html and the Truth in Lending Act.

[53] In fact, the large data breaches seen in 2008 and 2009 were a direct result of merchants not using encryption in their back-end systems, based on the (false) assumption that hackers would not be able to see this data in transit.

C. The cloud computing industry suffers from market failure

If cars did not come with locks, the market would soon provide an incentive for manufacturers to add them. Once vehicle owners came back from a night out on the town and discovered that their car was missing, these theft victims would soon tell their friends, and make certain to demand locks from the dealer during their next purchase.

The situation is radically different in the cloud computing industry. First, consider that if a consumer's car is stolen, they usually learn of the theft rather promptly, as the car will be missing when they next attempt to use it. The theft or unauthorized access to an online account is different, since both the thief and the legitimate owner can concurrently access the same cloud based resource. That is, the user can continue to create and edit documents, while the thief is able to read each new memo and spreadsheet as they are created. The online account, unlike the stolen car, is a non-rivalrous good.[54] As a result, users of most cloud based services are not able to use this valuable signal that something bad has happened.[55]

Second, once consumers do find out that their accounts have been hacked into, they are often not able to identify the event that lead to hackers gaining unauthorized access. While a shattered car window will reveal how a thief broke into the vehicle in order to steal a stereo, there is no tell-tale evidence left behind when a hacker snoops on an insecure cloud session in a coffee shop or other public place.

Most users of cloud computing services are unaware of the following:

1. Their private information is insecurely transmitted over the network,
2. That widely available technologies exist to provide for that secure transmission,
3. That the cloud service providers have opted to not deploy such safeguards and
4. That off-the shelf tools exist which can be used by hackers to easily break into their private email accounts and other cloud services.

Due to the widespread (yet understandable) ignorance of most end-users, it is not terribly surprising that all of the major cloud computing providers opt to ignore this security issue. There simply isn't sufficient market demand for these firms to allocate the considerable resources that would be required to deploy encryption, by default, for all of their products. In a highly competitive industry with razor thin per-customer profits, there is no incentive to needlessly dedicate computing resources to something for which most customers have not expressed a want.

Encryption can be thought of as a shrouded product attribute similar to the cost of printer ink refills, or hidden fees associated with "free checking" bank accounts.[56] Consumers rarely consider the full cost of these products, because they do not calculate in the added costs of these shrouded attributes. When most consumers evaluate a cloud computing service, they likely consider the usability, speed and perhaps weigh in social factors – such as the number

---

[54] That is, until the attacker changes the password, at which point, the user will be locked out. "Rival goods are goods whose consumption by one consumer prevents simultaneous consumption by other consumers." See: http://en.wikipedia.org/wiki/Rivalry_(economics)

[55] Google is an exception here, in that it provides gmail users with notice that another computer is currently logged into their account. No other services offer this feature.

[56] "[C]onsumers sometimes fail to anticipate contingencies. When consumers pick among a set of goods, some consumers do not take full account of *shrouded product attributes*, including maintenance costs, prices for necessary add-ons, or hidden fees …. Shrouded attributes may include surcharges, fees, penalties, accessories, options, or any other hidden feature of the ongoing relationship between a consumer and a firm." See: Shrouded Attributes, Consumer Myopia, and Information Suppression in Competitive Markets, http://www.econ.yale.edu/~shiller/behmacro/2003-11/gabaix-laibson.pdf

of their friends who are currently using it. Consumers are unlikely to consider the encryption offered (or not) by the service, particularly since most are not even aware of the existence of encryption when it is offered.[57]

In their seminal work analyzing markets with shrouded attributes, Gabaix and Laibson reveal that these goods can lead to two forms of exploitation in the market: Optimizing firms exploit myopic consumers through marketing schemes that shroud high-priced add-ons. In turn, sophisticated consumers exploit these marketing schemes. Simply put, by hiding the true cost of a product, a firm can offer the good at a lower initial price, since it will be able to recoup any lost profit via after-market sales. Savvy consumers can take advantage of this if substitute add-on goods (such as generic printer ink refills) are available. The paradox that Gabaix and Laibson identify is that this leads to a situation in which manufacturers have no incentive to ditch the shrouded good model, offer fairly priced goods, and advertise the evils practiced by their competitors. This is because each consumer educated about the shrouded attributes, rather than flocking to fair vendors, will instead purchase cheap after-market substitutes, and continue to purchase the subsidized shrouded good.

Given this economic theory, consider the market for encrypted cloud based services. Google offers SSL encryption for its services, but does not turn it on by default. If Google turned encryption on by default, its cost of offering the service to each customer would go up. Assuming that its profits did not, the company would either have to make do with less profit per customer, or more likely, reduce the cost of operating the service through other means. For example, Google could lower the amount of free disk space it provided to each customer.

Faced with choice between two cloud providers, one that encrypts all traffic but offers less storage, and a service which only offers encryption to users savvy enough to enable the option and more disk space, most savvy users would opt for the latter provider. In this situation, naïve users subsidize those more savvy, by enabling them to enjoy both encryption and large disk quotas.

Thus, when one provider offers this subsidized form of encryption, it creates a strong disincentive for other firms to go down the path of encryption by default. Such a firm will be unable to compete for naïve customers, since it will have lowered the amount of disk space and other features in order to pay for the encryption related costs. This firm will also be unable to attract the savvy customers, since these will flock to providers which offer both encryption as well as large amounts of disk space.[58]

D. Providing incentives for good security

The solution to the problem of excessive prices for after-market print supplies can be solved by requiring printer manufacturers to prominently advertise the price per page, thus making it easy for consumers to easily compare prices. In such a market with posted prices, printer manufacturers which sell higher printers with reasonably priced ink can compete with those which make use of shrouded ink prices.

A similar fix could be applied to the market for cloud based services – by requiring vendors to clearly disclose the risks of using their services without encryption. Given a sufficiently informed populace, the market should be able to take over, and firms may see the benefit in providing users an encrypted service given sufficient demand. Such a disclosure

---

[57] See generally, “The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies”, Stuart E. Schechter, Rachna Dhamija, Andy Ozment, Ian Fischer

[58] This theory at least explains why only Google offers encrypted mail, word processing and spreadsheets. As for why no social networks offer SSL, we are still scratching our heads.

requirement could take the form of a mandatory notice, placed on the login pages for each cloud based service which lacked SSL encryption. Examples of such a notice could include:

> WARNING: Email messages that you write can be read, intercepted or stolen by the person sitting next to you at Starbucks. If you wish to protect yourself from this risk, click here for a secure version of our service.
>
> WARNING: Email messages that you write can be read, intercepted or stolen by the person sitting next to you at Starbucks. This service does not provide the encryption necessary to protect you from this risk. However, other services do. Click here to see a list of these.

Such text would need to be prominently displayed, and not hidden deep within a web site's terms of service. However, Google's much publicized resistance to being forced to add any text to its website,[59] it is quite likely that the company would opt to bear the financial burden of enabling encryption by default, rather than clutter up its "beautiful clean home page."[60]

While such a desire to keep their home pages clutter free might not motivate other companies, the increase in consumer awareness of the risks made possible through such mandatory labeling, might provide enough of a push in market demand to nudge these firms into offering such product functionality.

An alternative approach, of course, would simply be for the government to regulate providers of cloud computing services, as it has already done in the banking and health industries. Banks are simply not permitted to let customers to make encryption a "choice," just as car manufacturers are no longer permitted to make seat belts optional. We would prefer that regulators first forced cloud computing providers to display clear educational warnings before regulators go down the path of mandating specific technologies. However, if educational warnings failed to provoke a sufficient market response, stronger regulation might be appropriate.

III. Personal privacy, cloud computing and the government

In the preceding section, we focused on threats to consumer privacy from private actors, mainly hackers and other evil-doers who are able to easily hijack and steal cloud based user data. In such a scenario the hacking happens without the knowledge or consent of the service provider, who would of course shut down such unauthorized access if it knew it was happening.[61]

This paper will now focus on an even more serious threat to end-user privacy – one without easy fixes. The primary focus will be on invasions of privacy in which the service provider is not only aware, but assists in the act, albeit due

---

[59] "Google believes so strongly that adding the phrase "privacy policy" to its famously Spartan home page would distract users that it has picked a fight with an advertising trade group over the issue … Larry Page, the company's co-founder, didn't want a privacy link `on that beautiful clean home page,' … 'His argument is when you come to Google and you are looking for information, it is that big fat box' for search and little else, the executive said." See: Google Fights for the Right to Hide Its Privacy Policy, http://bits.blogs.nytimes.com/2008/05/27/google-fights-for-the-right-to-hide-its-privacy-policy/

[60] See id.

[61] Our criticism in this section was focused on the cloud providers for not doing anything to stop the attacks from happening before the fact.

to coercion. In such cases, the surveillance occurs pursuant to a lawful order obtained by government agents,[62] and so even if the service provider wishes to protect its customers, it cannot.

The rest of this paper will progress as follows: It will first explore the changing market dynamics which have made large-scale surveillance of electronic communications both easy and cheap for the government. As a result, the marginal cost of watching one more person has now dropped to essentially nothing. It will then briefly explore the third party doctrine, which is the primary legal doctrine which the Government relies on to force the disclosure of user information held by third parties, neutralizing the traditional Fourth Amendment protection offered to people's personal documents and papers.

The solution to the privacy problems posed by the third party doctrine is actually rather simple – the mass deployment of encryption by software manufacturers and service providers. However, encryption alone is not the answer. This is due to government's lawful powers of coercion, through which it can compel service providers to insert back doors in to their own products, circumventing the encryption that would otherwise protect their customers' data. The core of this paper will focus on this issue, and the way that this power to force the insertion of back doors can be applied to the providers of cloud computing services.

A. The changing economics of surveillance

The mass adoption of digital technologies over the past decade has lead to a radical shift in the government's ability to engage in large scale surveillance.

Fifty years ago, if a government agency wished to monitor a suspect, it would have needed to dedicate a number of agents to engage in around the clock physical surveillance, have the post office intercept and divert her mail, which would be steamed open, itself a labor intensive task. If phone surveillance was required, someone would need to climb up a telephone pole or open an access panel attached to an apartment building in order to physically attach wires to the suspect's line. With the tap in place, agents would need to monitor the calls around the clock.[63] Finally, if

---

[62] In some cases, this may take the form of a warrant, but it may also be via a subpoena, or some other method in which there is little to no judicial oversight.

[63] In some cases, agents have turned to family members for help with this task. For example, in the famous Olmstead case it was a prohibition agent's wife who listened to the wiretaps in real time, took stenographic notes, and then prepared a transcript of the conversation which federal agents later relied upon for their own testimony. "But the record shows that the witness testified only to conversations which he heard over the wire, and that he used the typewritten book only to refresh his memory. He was asked whether he wrote the entries. He answered that he saw them written, part of them at the time when the conversations were heard, part of them two or three days later; that his wife made all of the entries in the book; that she made stenographic notes of the conversations at the time thereof, and the witness testified that he had an independent recollection of the conversations." See: Olmstead v. United States, 19 F.2d 842; 1927 U.S. App.

In the dissent, Judge Rudkin stated that "the witnesses were unable to testify without having in their hands the copied data to which they could refer for facts which they could not remember; they had no independent recollection thereof. True, they had a general recollection of events to which the data pertained, but they had to resort to those notes for dates and names and persons, and the quantities and kinds of liquor purchased … if they needed to refer to their records only to arouse a present recollection, the reading of the original records and the making of notes there from would have fully served the purpose. It would not have been necessary for them to hold in their hands the copied notes and refer to them while they were giving testimony. In the present case, witness after witness, day after day, testified to names, dates, and events, so numerous and with such unerring accuracy, that it becomes at once apparent that the book, and not the witnesses, was speaking. A better opportunity to color or fabricate testimony could not well be devised by the wit of man."

investigators wished to learn the contents of conversations spoken inside the home, a hugely laborious and risky "black bag job" would be necessary, in which highly skilled agents would break into the suspect's residence or workplace to covertly install microphones and remote transmitters.[64]

Times have changed. Telecommunications companies and Internet Service Providers now have dedicated legal compliance departments,[65] some open 24 hours per day, through which law enforcement agents can obtain wiretaps, emails, text messages or real time phone location information. Once contacted, service providers can enable a wiretap with a few keyboard strokes – without the need to enter the customer's home or even manually connect wires in a switching center.

Once the wiretap has been initiated, the customer's data gets automatically transmitted to the government servers. While this typically happens on a case-by-case basis, it appears that at least one telecommunications company has given the FBI wholesale access to its entire network, enabling agents to tap customers at will without requiring that the company's staff enable or assist with the surveillance.[66] Similarly, multiple Internet service providers have been accused of providing raw access to their "backbone" networks to the National Security Agency, which was then free to target individual communications for surveillance without the need to involve the communications company.

Even just 5 years ago, if the government had wanted to get access to potentially incriminating evidence from the home computers of ten different suspects, investigators would have needed to convince a judge that they had probable cause in order to obtain a search warrant for each person. They would then have sent agents to raid the homes of the individuals, remove the computers, and then later perform labor-intensive forensic analysis in order to get the files. In the event that the suspects knew each other, the government might opt to perform a simultaneous raid (thus requiring even more manpower), so that one suspect could not notify the others – who might then delete their files.

Now that many users have switched to cloud based services, digital search and seizure has become far easier. Law enforcement agencies can essentially deputize the technology companies that provide applications to end users, and make these firms part of the surveillance infrastructure. The private documents of ten individuals can now be

---

[64] "Since 1948 the FBI has conducted hundreds of warrantless surreptitious entries to gather domestic and foreign intelligence, despite the questionable legality of the technique and its deep intrusion into the privacy of targeted individuals. Before 1966, the FBI conducted over two hundred `black bag jobs.' These warrantless surreptitious entries were carried out for intelligence purposes other than microphone installation, such as physical search and photographing or seizing documents. Since 1960, more than five hundred warrantless surreptitious microphone installations against intelligence and internal security targets have been conducted by the FBI, a technique which the Justice Department still permits. Almost as many surreptitious entries were conducted in the same period against targets of criminal investigations … Surreptitious entries were performed by teams of FBI agents with special training in subjects such as `lock studies.'" Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Final Report: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans, Book III, S. Rep. No. 94-755, at 355 (1976)], available at http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIIf.htm

[65] See generally a list of the legal compliance departments at hundreds of phone/Internet companies: "ISP List", http://www.search.org/programs/hightech/isp/. See also: http://www22.verizon.com/ResidentialHelp/Phone/General+Support/Support+Tools/General/122857.htm and

[66] "Because the data center was a clearing house for all Verizon Wireless calls, the transmission line provided the Quantico recipient direct access to all content and all information concerning the origin and termination of telephone calls placed on the Verizon Wireless network as well as the actual content of calls." See: http://blog.wired.com/27bstroke6/2008/03/whistleblower-f.html

obtained through a single subpoena to Google – whose engineers will then locate the files (stored on the company's servers) and provide them to the government.

This approach obviously has many benefits to law enforcement: significantly reduced manpower requirements, no need to go before a judge or establish probable cause in order to obtain a warrant, as well as the complete elimination of physical risk to agents who might be shot or attacked in the during a raid.

B. Surveillance at near zero marginal cost

Modern surveillance technology is notable for the fact that the vast majority of the cost of systems is for up-front infrastructure. Intelligence and law enforcement agencies must purchase data centers filled with expensive computer equipment, and then develop custom software for initiating, recording, cataloging and indexing the wiretaps.[67] The government has required that telecommunication companies upgrade to modern digital switches with CALEA mandated intercept capabilities and provided hundreds of millions of dollars to help pay for this.[68]

Once these up front or predictable fixed costs (such as salaries for agents and lawyers) have been paid for, modern surveillance is surprisingly cheap, if it costs anything at all. In some cases, telecommunications companies and ISPs may charge to initiate and continue surveillance, in others, they may provide the information for free.

To those companies that do charge, surveillance can be a profit center.[69] A $50 per month home Internet connection can lead to hundreds of dollars in additional revenue when that customer is wiretapped.[70] However, in the event that a telecommunications company provides the government unfettered access to its backbone network,[71] wiretaps are essentially free – since the equipment, leased data lines and agent manpower would be paid for no matter how many individuals are being watched.

With the surveillance infrastructure in place, all that law enforcement agents need to do is to issue a couple commands from a computer terminal, at which point, a government server will begin capturing a suspect's raw telephone, Internet and other traffic. Automated software can scan the contents of the calls and emails, and a summary report can be sent to an agent if there are any matches. The interception itself requires little to no direct supervision, and so it is just as easy to tap 1, 50 or 100 additional suspects.

C. The problem with free and cheap surveillance

---

[67] FIXME – add carnivore stuff here.

[68] The FBI paid Verizon $2500 a piece to upgrade 1,140 old telephone switches, See: http://blog.wired.com/27bstroke6/2008/05/secret-data-in.html

[69] See generally, Andrew Appel, "Eavesdropping as a Telecom Profit Center", Freedom To Tinker Blog, http://freedom-to-tinker.com/blog/appel/eavesdropping-telecom-profit-center

[70] Comcast charges $1000 setup for each new tap (this includes the first month free): http://www.fas.org/blog/secrecy/2007/10/implementing_domestic_intellig.html

[71] See, FIXME Verizon earlier. See also AT&T secret room in San Francisco.

Telecommunication companies often act as a form of oversight for surveillance requests. In several past instances, companies have refused to comply with surveillance orders that they believed were illegal.[72] Federal wiretapping laws outlines specific civil liabilities for companies that provide customer information without meeting the appropriate legal requirements. This liability gives telecommunication companies a strong incentive to insist that the law is being followed. Thus, when wiretaps can be performed without any involvement of the telecommunication providers, consumers are denied this crucial additional layer of oversight, and must rely upon law enforcement and intelligence agencies to not abuse their access.

Another spillover benefit of the pay-for-surveillance model is that it creates a paper-trail. That is, if the government is billed for each wiretap it requests, a billing record will be generated detailing the date that tap began, ended, the number or customer tapped, as well as the cost of this service. At least two copies of this will be generated, one for the ISP and another sent to the investigating agency. This paper trail provides a wealth of data for oversight bodies, and the fear of creating such a paper trail may dissuade investigators from initiating surveillance without the appropriate evidence.

Finally, per-transaction-billing based surveillance brings the benefit of scarcity. That is, given a fixed size budget, and a practically endless number of possible suspects, government agents are forced to prioritize their surveillance efforts. This provides a strong incentive for them to focus on investigations likely to bear fruits, as well as to stay away from "fishing expeditions."

Even in the event that a provider charges for surveillance assistance, this situation is still much better for government agents than in the pre-digital days. Sending agents out to monitor a home or trail a suspect consumes significantly more resources than paying an ISP $1000 to turn on a wiretap or locate a mobile phone. It is also much safer.

Obtaining and serving a warrant upon a suspect, raiding her home, and seizing her computers not only consumes valuable agent hours,[73] but it places agents in harm's way. A suspect could be armed, or have protected his home with booby traps. While law enforcement agencies might mitigate this risk through the use of SWAT style tactics, the risk to their own is still there. This risk of physical harm provides an additional and highly personal incentive for officers to limit such searches. However, now that cloud computing companies are able to provide law enforcement with the documents that would have once required an armed raid, this risk of physical harm is gone, and with it, whatever disincentives for over-reach it provided.

D. Cloud providers and the third-party doctrine

The Fourth Amendment guarantees all Americans a measure of control around their bodies and possessions that the government cannot enter or search without reasonable cause. Thus, your diary, your personal letters, and other such property are normally provided with constitutional protection. Americans have become used to these rights, and

---

[72] Cite: Qwest, onstar, FISA/Protect America Act Court order from 2008,

[73] Warrants are costly to the police: they require both paperwork and hours hanging around a courthouse waiting to see the magistrate … Both the warrant and probable cause requirements, then, make house searches considerably more expensive for police than those searches would be absent those requirements. The rules function as a tax, payable in police time rather than money. When a police officer decides to search a house or apartment, he must first spend several hours performing tasks that the law says are prerequisites to such a search … if you tax a given kind of behavior, you will probably see less of it." See: William J. Stuntz, The Distribution of Fourth Amendment Privacy, 67 Geo. Wash. L. Rev. 1265 (1998-1999)

often take for granted that private matters are usually kept private. Unfortunately, as we have move to communicating and working online, our constitutional protections have been left behind.

Fourth Amendment protections against unreasonable search and seizure depend upon a person's reasonable expectation of privacy. Unfortunately for users of Internet based services, existing case law does little to protect their digital documents and papers which are now increasingly being stored on the remote servers of third parties.

The cause of this departure from the Fourth Amendment: the third party doctrine, which establishes that people have no expectation of privacy in the documents they share with others. Rather than revisit *Smith v. Maryland* and *United States v. Miller* at length, a single quote from the Supreme Court should be enough:

> "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed to him by Government authorizes, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[74]

The third party doctrine is the "Fourth Amendment rule that scholars love to hate," "widely criticized as profoundly misguided", and decisions applying the doctrine "top[] the chart of [the] most criticized Fourth Amendment cases."[75] However, for the purposes of this article, it is enough to simply state that online service providers can be compelled to reveal their customers' private documents with a mere subpoena.[76] The government is not required to obtain a search warrant,[77] nor must they demonstrate probable cause.[78]

While the third party doctrine is certainly the current tool of choice for the government's evisceration of the Fourth Amendment, is not completely to blame. In fact, as we will later argue, the rule actually provides some potential incentives for service providers to protect their customers' privacy. The real and often overlooked threat to end-user privacy is not this legal rule, but the industry-wide practice of storing customers' data in plain text, forgoing any form of encryption.

Simply put, if encryption were used to protect user's stored data, the third party doctrine would be a moot point. Thus, the question we must now focus on is the failure of the market to provide end-users with this crucial protection from warrantless government intrusion.

---

[74] United States v. Miller

[75] Kerr, The Case for the Third Party Doctrine

[76] For example, see GOOGLING AWAY YOUR PRIVACY: PROTECTING ONLINE SEARCH INQUIRIES FROM UNWARRANTED STATE INTRUSION, noting that Google was compelled to produce two months worth of search records in response to a government subpoena.

[77] "Because ISPs are third parties, and usually corporate entities at that, the government will not ordinarily search the servers of ISPs directly. The government will instead seek a court order compelling the network provider to disclose the information to the government. This is important because the Fourth Amendment generally allows the government to issue a grand jury subpoena compelling the disclosure of information and property, even if it is protected by a Fourth Amendment `reasonable expectation of privacy.'" See: Orin Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, at page 5.

[78] "When the government obtains a court order such as a subpoena that requires the recipient of the order to turn over evidence to the government within a specified period of time, the order will generally comply with the Fourth Amendment if seeks

relevant information and is not overbroad.12 No probable cause is required.", See Orin Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, at page 5.

E. Why we don't have widespread encrypted cloud services

For the purposes of this section, we differentiate between different types of of encryption: Network encryption (typically SSL) used to protect data as it is transmitted from the client to a server, and data encryption, which is used to protect the data once it is in storage. Within this latter category, we further differentiate between two forms: data encryption in which the service provider knows the encryption key, and data encryption in which the service provider does not know the encryption key.

Network encryption only protects data in transit, and so the use of this technology does nothing to protect users' data from a subpoena. Likewise, if a cloud provider has both the user's data, and the key used to encrypt it, it can be compelled to produce both. The only real protection from the government comes with the encryption of data with a key that only the user knows.

As we will now argue, there are two main reasons why most cloud providers have not gone down this path.

F. A lack of perceived consumer demand for encryption of stored data

As explained earlier in this paper, network encryption can protect user data against from passive attackers who might sniff data as it is transmitted from the customer's computer to the cloud provider. Encryption of the data in storage protects against a totally different set of threats. If the service provider knows the encryption key, the user still gains significant protection from data loss risks – that is, misplaced backup tapes and stolen laptops, providing the company is not storing the encryption key on the same media as the encrypted user data.

Data encryption with a key that is private to the user protects against a very specific set of attacks – so called insider attacks, where an employee "peeks" at customer data, and legally compelled disclosure. As we will now argue, these are two potential risk scenarios which companies have little to no incentive to publicize. Simply put, service providers would prefer if their customers did not know these risks existed.

While it is little known to most consumers, government requests to Web 2.0 companies have become a routine part of business. All cloud computing providers now have dedicated legal compliance departments,[79] some open 24 hours per day, through which law enforcement agents can obtain emails, search records and other stored customer data. While Google has widely publicized its initial refusal to deliver search records in response to a request by the US Department of Justice in 2006, it has been far less willing to discuss the huge number of subpoenas it receives per year, to which it does comply and thus deliver its customers' data to law enforcement agencies.[80] Of course, Google is not alone in not wishing to discuss this – there seems to be a conspiracy of silence amongst the entire industry.[81]

---

[79] See generally a list of the legal compliance departments at hundreds of phone/Internet companies: "ISP List", http://www.search.org/programs/hightech/isp/. See also: http://www22.verizon.com/ResidentialHelp/Phone/General+Support/Support+Tools/General/122857.htm and

[80] "The new policy also shouldn't affect many investigations, [Google Deputy Counsel Nicole] Wong said, since the two year time limit 'seems to be at the outer edge of what police want.' Mostly police are interested in logs that are a day or two old, according to Wong. Google still refuses to disclose how often their logs are subpoenaed, even in cases where they are free to do so." See: http://www.wired.com/threatlevel/2007/03/google_to_anony/

Even with this silence, it would be wrong to assume that consumers do not care the ease with which their private information can be disclosed. For example, in early 2009, Sweden passed a new law requiring Internet Service Providers to hand over customer's information to intellectual property holders investigating piracy. Swedish Internet traffic dropped by over 30% starting the day that the new law came into effect.[82] This clear demonstration of consumer's privacy fears then lead to competition in the market for privacy-preserving services. Within weeks, three of Sweden's Internet Service Providers had announced new policies in which they would not retain any information linking IP address information to particular 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."[83]

There is one significant difference between most cloud computing providers and the Swedish ISPs who responded to consumer demand for privacy: Money. The Swedish ISPs' primary source of revenue is the monthly fees which they charge their customers for broadband Internet services. However, the cloud computing providers generally provide their services for free, and make their money by collecting large amounts of consumer data, which they then monetize by selling advertising. While the ISPs can easily afford to do without detailed consumer data, the cloud computing providers, at as their business models currently stand, cannot. Their profit margins depend upon their ability to convince customers to trust them with *more* private data, not less.

G. Business models that depend on advertising and data mining

---

"Does Google keep records on how data which it has retained and provided to authorities is used? For example, in this case the data was used to conduct a raid and seizure of a computer lab and newspaper. In other countries there could be other (worse) ramifications due to human rights problems. Of course in many cases Google's data and cooperation could aid the investigation of a crime, from financial fraud to stalking.

GOOGLE: As a matter of policy, we don't comment on the nature or the substance of law enforcement requests to Google." See: http://www.indybay.org/newsitems/2008/09/10/18534988.php

"How many subpoenas for server log data does Google receive each year?

As a matter of policy, we don't provide specifics on law enforcement requests to Google" See: Google Log Retention FAQ, www.seroundtable.com/google_log_retention_policy_faq.pdf

[81] "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." 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." See: ISP responses to CNET News Survey, http://news.cnet.com/8301-13578_3-9962106-38.html

[82] 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 … traffic fell from an average of 120Gbps to 80Gbps on the day the new law came into effect." See: http://news.bbc.co.uk/2/hi/technology/7978853.stm

[83] http://news.cnet.com/8301-1023_3-10229618-93.html

It is exceedingly difficult to monetize a data set that you cannot look at. Google's popular Google Mail 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 were encrypted with a key not known to Google, the company would be unable to scan the contents and display related advertising. Sure, the company could display generic banner advertisements unrelated to the user's activity, but these would earn the company far less revenue.[84]

Google's Docs service, Adobe's Photoshop Live, Facebook, and MySpace are all provided for free. Google provides its users with gigabytes of storage space, yet doesn't charge a penny for the service. These companies are not charities, and the data centers filled with millions of servers required to provide these services cost real money. The companies must be able to pay for their development and operating costs, and then return a profit to their shareholders. Rather than charge customers money, the firms have opted to monetize their user's private data. As a result, any move to protect this data will directly impact the companies' ability to monetize it, and turn a profit.[85] Simply put, advertising based business models are incompatible with private key encrypted online data storage services.

Advertising is not the only way to profit from cloud computing. In recent years, Google has begun to offer its "Apps for Domains" product, in which it provides Mail, Docs, Spreadsheets and other cloud based services to companies, universities, and governments. Google does not mine these corporate customers' email for advertising purposes, and instead charges $50 per user per year, which is more than enough to pay for the service and make a profit. Likewise, Microsoft offers its Office Live based suite to corporate customers wishing to pay a per user fee. If customers, particularly those in the corporate and government space were willing to pay for the higher development and computational costs required for encryption, it is quite likely that companies like Google and Microsoft might compete to meet the market demand.

H. Encryption in the cloud

Cloud based services do have to put the privacy of their users at risk. Consider, as an example, the Weave Firefox browser-add on produced by Mozilla Labs.[86] This tool enable users to keep their bookmarks, browsing history, saved passwords, and cookies synchronized across multiple computers. Users can, when at work, easily find a Web page they had been viewing the night before at home. The tool even support's Mozilla mobile phone browser, allowing users to bookmark a Web page at work and then later view it while commuting to work from their phone.

Like all cloud services, Mozilla achieves this instant, worldwide access by allowing users to store their own data on Mozilla's servers. However, Mozilla baked privacy into the product at the design stages, stating that a key principle of the project that "users own their data, and have complete control over its use. Users need to explicitly enable third

---

[84] In fact, it is the higher click through rates and higher cost per click that have lead Google and many other online companies to push heavily into the behavioral/targeted advertising space, in which increasingly large amounts of data are collected about users' activity online.

[85] "If Google can build a higher–quality data set of customer information, they can charge more per advertisement, whilst also gaining a significant market advantage over the other search engines." Christopher Soghoian, "The problem of anonymous vanity searches" at http://ssrn.com/abstract=953673.

[86] Introducing Weave, Mozilla, Dec. 12, 2007, available at http://labs.mozilla.com/2007/12/introducing-weave

parties to access their data."[87] As a result, the data that Weave 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 attempt to compel Mozilla to share its users' Weave data, the company can confidently hand over the encrypted files with the knowledge that the data is complete gibberish to everyone but the user.

Of course, Mozilla is not attempting to monetize the Weave service, which is perhaps why it has been free to put user privacy first. It has even provided an open source Weave server, so that other groups and companies can provide their own cloud-based storage for Weave users.

Let us now imagine a situation in which Google, Microsoft and the other providers followed Mozilla's example, and built strong encryption into their own services, such that only the users would have the ability to decrypt their own data.

In this hypothetical scenario, Google's Docs word processor would store each user's files in an encrypted form on Google's vast array of servers. When the user loaded the Google Docs application in their Web browser, it would prompt the user for her password. The Web application would then request copies of the most recent documents from Google's servers, download them, and then decrypt these files locally in the browser. As the user made changes to the documents, the modifications would be encrypted, and then transmitted to Google's servers. Users would still be able to access their own documents from any computer around the world, yet the documents would be safe from the prying eyes of governments, divorce lawyers, and even inquisitive rogue Google employees.

Such a scenario is not beyond the realm of imagination. Certainly, as Mozilla's Weave has demonstrated, it is technically possible. Were the industry to follow Mozilla's example and encrypt all user data, the intrusions upon end-user privacy made possible by the third party doctrine would largely be neutralized.

I. How encryption would change the status quo

A move to encrypted cloud based services would likely lead to a significant reduction in the ease with which law enforcement agents could obtain the private files of suspects. We consider this to be a feature, not a bug. Simply put, cloud computing and the online storage of data by third parties has made law enforcement far too cheap. It is time for a market adjustment.

Nevertheless, pro-law enforcement types might argue that without the ability to force service providers to reveal their customer's communications, law enforcement would be unable to engage in the lawful investigation of criminal suspects.

While we certainly wish to roll back the effectiveness, scale and extreme low cost at which the government can currently engage in surveillance, we do recognize that there is a legitimate need to investigate suspects. Luckily, even with the widespread use of encryption, there is still a way for law enforcement to get access to data: the black bag job.

As noted earlier in this paper, in the days before easy taps at the phone company, law enforcement would have to send an agent out to tap the line at the suspect's home, or perhaps scale a nearby telephone pole. Encryption rolls us back to this style of manual labor in placing wiretaps. The recent *Scarfo* case provides a fantastic example of this, in

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

which a suspect's use of disk encryption was defeated by the FBI. A team of agents snuck into Scarfo's home, planted microphones and other recording devices in his computer, which then captured a copy of his password as he typed it on the keyboard.[88] No matter how strong the encryption, the human is always the weakest link, and the black bag job exploits this.

What we propose is not the end to the lawful acquisition of investigative data, merely that law enforcement no longer be able to deputize service providers into stealing their customer's data. If a suspect is important enough, let the police dedicate the significant manpower to break into her home in order to install bugs. Given the finite limit to the financial and human resources available to law enforcement agencies, such a change in the balance of power, by raising the effective cost of such surveillance, would force investigators to prioritize their targets, and shy away from fishing expeditions.[89]

Furthermore, such a switch would also bring a further (and significant) benefit to privacy activists: The return of the Fourth Amendment. If police needed to break into a suspect's home in order to try and install a password-stealing bug, they would first have to obtain a search warrant, and thus find themselves firmly back in the familiar domain of the Fourth Amendment. This would lead to at least some judicial oversight of investigations, something that is not currently necessary when data can be obtained with a subpoena.

As much as a move to encryption would cheer up privacy activists and cypherpunks, encryption technology is not a magic bullet. As we will now explain, even if cloud computing providers deployed encryption, the government has a powerful trump card: the ability to force service providers to insert back doors into their own products.

IV. Companies can be forced to turn against their customers

When consumers purchase technology, it is typically because they want to perform some task or function. It is exceedingly unlikely that purchases are made with the goal of making it easier for the government to spy on the purchaser. However, that scenario actually plays out in real markets, with real products. In the vast majority of cases, the consumer never knows it.

Consumers have significantly reduced privacy rights when they are spied upon with their own devices and software. For example, while government agents have to jump through significant hoops to place tracking devices on a suspect's vehicle, that same suspect's mobile phone can be made to report its location with far less paperwork. Furthermore, even if a company attempts to build privacy-protections into its products, these can be neutralized. Technology providers are frequently forced to circumvent their own privacy protections and insert backdoor their own products – adding new functionality whose sole purpose is to harm the privacy of the customer. We now present a few examples of this.

---

[88] See generally: *Re: United States v. Nicodemo S. Scarfo, et al, 180 F. Supp. 2d 572; 2001 U.S. Dist.*

[89] "Where there are more crimes than the police can investigate, the police must, by definition, choose which crimes to investigate. Anything that makes investigating some crimes more expensive will tend to drive police toward other crimes, in the same way that making airplane travel more expensive will drive passengers to trains or cars … Some police tactics are wholly unregulated, some are regulated lightly, and a few, like house searches, are regulated fairly heavily. In a world like that, a world where the law taxes some kinds of policing more than others, the likely substitutions will occur within policing, not outside it, as the police shift time and energy away from more expensive (because more highly taxed) tactics and toward cheaper ones." See: William J. Stuntz, The Distribution of Fourth Amendment Privacy, 67 Geo. Wash. L. Rev. 1265 (1998-1999)

A. The FBI's Magic Lantern / Computer and Internet Protocol Address Verifier (CIPAV)

In 2001, it was revealed that the FBI had developed a malicious software suite for the purpose of stealing information from suspects' computers.[90] The "Magic Lantern" tool (since renamed the Computer and Internet Protocol Address Verifier or CIPAV) has much in common with typical computer viruses – that is, the FBI relied upon un-patched vulnerabilities in a suspect's computer to gain access and then covertly install their software tool. However, instead of sending a victim's private documents back to a would-be identify thief in Eastern Europe, the personal files were instead sent to a FBI computer in Quantico, Virginia.[91]

All available information on the use of CIPAV seems to indicate that the tool is only used after law enforcement officers have obtained a search warrant. However, the revelation of the tool's existence did lead to a significant tech media firestorm when Network Associates reportedly told the Associated Press that the company would be willing to modify its popular McAfee Anti-Virus software suite to ignore the FBI's own spyware software.[92] That is, customers who purchased the anti-virus suite would not be warned if their computers were infected by an FBI-written virus.

In a 2007 survey of 13 anti-spyware vendors, all of the companies stated that their policy was to detect all forms of spyware, including software made by the government.[93] However, when asked if they had ever received a court order requiring the white-listing of government spyware, both Microsoft and Network Associates declined to comment.[94]

---

[90] http://www.villagevoice.com/2002-05-28/news/the-fbi-s-magic-lantern/1

[91] "The full capabilities of the FBI's "computer and internet protocol address verifier" are closely guarded secrets, but here's some of the data the malware collects from a computer immediately after infiltrating it, according to a bureau affidavit acquired by Wired News: IP address; MAC address of ethernet cards; A list of open TCP and UDP ports; A list of running programs; The operating system type; version and serial number; The default internet browser and version; The registered user of the operating system, and registered company name, if any; The current logged-in user name; The last visited URL …. All that information is sent over the internet to an FBI computer in Virginia, likely located at the FBI's technical laboratory in Quantico." See: FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats, http://www.wired.com/politics/law/news/2007/07/fbi_spyware?currentPage=all

[92] "Network Associates has been snared in a web of accusations over whether it will place backdoors for the U.S. government in its security software …. An Associated Press article then reported that 'at least one antivirus software company, McAfee Corp., contacted the FBI ... to ensure its software wouldn't inadvertently detect the bureau's snooping software and alert a criminal suspect.'" See: http://www.wired.com/politics/law/news/2001/11/48648

[93] "Some companies that responded to the survey were vehemently pro-privacy. 'Our customers are paying us for a service, to protect them from all forms of malicious code,' said Marc Maiffret, eEye Digital Security's co-founder and chief technology officer. 'It is not up to us to do law enforcement's job for them so we do not, and will not, make any exceptions for law enforcement malware or other tools.' See: http://news.cnet.com/Will-security-firms-detect-police-spyware/2100-7348_3-6197020.html

[94] "'Microsoft frequently has confidential conversations with both customers and government agencies and does not comment on those conversations,' a company representative said. Of the 13 companies surveyed, McAfee was the other company that declined to answer … Cris Paden, Symantec's manger of corporate public relations, initially declined to reply. 'There are legitimate reasons for not giving blanket guarantees--one of those is a court order,' he said at first. 'There are extenuating circumstances and gray issues.'" See: http://news.cnet.com/Will-security-firms-detect-police-spyware---page-2/2100-7348_3-6197020-2.html?tag=mncol

B. Mobile phones as roving bugs

In 2006, it was revealed that the FBI is able to remotely enable the microphones of mobile phones. This technique, called a 'roving bug' in court documents, enables the FBI to remotely instruct a mobile phone to turn on its microphone, and silently transmit the recorded audio back to government agents, all without notifying the user.[95] The feature has been used against two alleged mafia kingpins, who had been careful to avoid saying anything incriminating when making calls using their mobile phones. They were not so careful when they believed that the phones were off.

While it is unclear how the government is able to remotely enable the microphones, most experts point to a software update of some kind.[96] If an update is used, it is even more unclear how the software is being covertly installed onto the suspect's phone – that is, if the government is exploiting an un-patched vulnerability in the phone's software, or if federal agencies have been able to obtain the assistance of wireless phone companies or the device manufacturers themselves – most of whom have refused to discuss the matter.[97]

C. In-car navigation systems

In 2003, the 9th Circuit Court of Appeals ruled that providers of in-car navigational/GPS services could be forced to secretly enable their microphones without a customer's knowledge and remotely wiretap them.

This case relates to the use of in-car navigation systems with built in cellular data service. These products enable a customer to press a button in their vehicle to call for help whenever they get lost, and further provide for added safety functionality – such as the ability automatically call an ambulance whenever the car has an accident.[98] These

---

[95] "The FBI appears to have begun using a novel form of electronic surveillance in criminal investigations: remotely activating a mobile phone's microphone and using it to eavesdrop on nearby conversations … Nextel and Samsung handsets and the Motorola Razr are especially vulnerable to software downloads that activate their microphones, said James Atkinson, a counter-surveillance consultant who has worked closely with government agencies. 'They can be remotely accessed and made to transmit room audio all the time,' he said. 'You can do that without having physical access to the phone.'" See: "FBI taps cell phone mic as eavesdropping tool", http://news.zdnet.com/2100-1035_22-150467.html

[96] "But other experts thought microphone activation is the more likely scenario, mostly because the battery in a tiny bug would not have lasted a year and because court documents say the bug works anywhere "within the United States"--in other words, outside the range of a nearby FBI agent armed with a radio receiver. In addition, a paranoid Mafioso likely would be suspicious of any ploy to get him to hand over a cell phone so a bug could be planted. And Kolodner's affidavit seeking a court order lists Ardito's phone number, his 15-digit International Mobile Subscriber Identifier, and lists Nextel Communications as the service provider, all of which would be unnecessary if a physical bug were being planted." See: http://news.zdnet.com/2100-1035_22-150467.html

[97] "Verizon Wireless said only that it 'works closely with law enforcement and public safety officials. When presented with legally authorized orders, we assist law enforcement in every way possible.' A Motorola representative said that 'your best source in this case would be the FBI itself.' Cingular, T-Mobile, and the CTIA trade association did not immediately respond to requests for comment." See: http://news.zdnet.com/2100-1035_22-150467.html

[98] "The System automatically contacts the Company if an airbag deploys or the vehicle's supplemental restraint system activates." See: In the Matter of the Application of the UNITED STATES FOR AN ORDER AUTHORIZING THE ROVING INTERCEPTION OF ORAL COMMUNICATIONS, The Company v. UNITED STATES of America, 349 F.3d 1132.

systems only permit those inside the vehicle to call one of three preset numbers to call centers for emergency response, direction assistance and vehicle towing services. These services are typically pre-installed by car manufacturers, who also install microphones in the vehicles – permitting the customer to speak to call center workers when their assistance is needed.

While there was little to be gained by wiretapping a customer's calls to the emergency response call center staff, the FBI took an interest in the microphones pre-installed in many luxury vehicles, and the cellular transmission capabilities of the in-car navigational systems. Simply put, FBI agents sought to covertly enable the microphone without a suspect's knowledge, and then use the existing cellular capabilities in the system to snoop on in-car conversations.[99]

In making its argument, The Company cited the legislative history of the Communications Privacy Act of 1996, which seems to clearly prohibit wiretap orders that "require a company to actually accomplish or perform the wiretap" or where "wiretap activity take place on …. company premises."[100] The court dismissed this argument, contrasting between telephone wiretaps mentioned in the Congressional Record in which "law enforcement is familiar with the technology and needs only access to wires remote from the carrier's premises" and the in-car microphone example, where "the FBI cannot intercept communications in the vehicle without the Company's `facilities [or] technical assistance.'"[101]

While the Court believed that the FBI certainly had the legal authority to order The Company to turn its own technology against its customers, the FBI's requests were still ruled to be invalid. Pointing to the *minimum of interference* language in §2518, the Court stated that "the obligation of private citizens to assist law enforcement, even if they are compensated for the immediate costs of doing so, has not extended to circumstances in which there is a complete disruption of a service they offer to a customer as part of their business." Due to the fact that The Company's ability to provide services to customers under surveillance was severely restrained,[102] the Court ruled that the FBI's order was improper.

---

[99] "Upon request by the FBI, the district court issued several ex parte orders pursuant to 18 U.S.C. § 2518(4), requiring the Company to assist in intercepting oral communications occurring in a certain vehicle equipped with the System." See: In the Matter of the Application of the UNITED STATES FOR AN ORDER AUTHORIZING THE ROVING INTERCEPTION OF ORAL COMMUNICATIONS, The Company v. UNITED STATES of America, 349 F.3d 1132.

[100] "[Title III] should not be construed as authorizing issuance of an order for land line telephone company assistance which either requires a company to actually accomplish or perform the wiretap or requires that law enforcement wiretap activity take place on land line telephone company premises." S.Rep. No. 99-541, at 29-30 (1986).

[101] "In contrast to standard land line wiretaps, the FBI cannot intercept communications in the vehicle without the Company's 'facilities [or] technical assistance.' Since such hands-on assistance is necessary, assistance may be mandated by an order under § 2518(4). *Cf.* S.Rep. No. 99-541, at 29 (recognizing that cellular service providers allow law enforcement to use their premises and that Congress did not intend to alter this arrangement with any of its 1986 amendments to title III)." See: In the Matter of the Application of the UNITED STATES FOR AN ORDER AUTHORIZING THE ROVING INTERCEPTION OF ORAL COMMUNICATIONS, The Company v. UNITED STATES of America, 349 F.3d 1132.

[102] "In this case, FBI surveillance completely disabled the monitored car's System. The only function that worked in some form was the emergency button or automatic emergency response signal. These emergency features, however, were severely hampered by the surveillance: Pressing the emergency button and activation of the car's airbags, instead of automatically contacting the Company, would simply emit a tone over the already open phone line. No one at the Company was likely to be monitoring the call at such a time, as the call was transferred to the FBI once received. There is no assurance that the FBI would be monitoring the call at the time the tone was transmitted; indeed, the minimization requirements …. preclude the FBI from listening in to conversations unrelated to the purpose of the surveillance. Also, the FBI, however well-intentioned, is not in the business of providing emergency road services, and might well have better things to do when listening in than

While the 9th Circuit's decision protected customer privacy in this particular case, the Court left a clear path for compelled assistance with covert surveillance if it did not hamper a company's ability to provide service to its customers. If anything, this "victory" for the privacy community was extremely hollow.

D. Torrentspy

In 2006, Torrentspy, a popular peer-to-peer filesharing search engine was taken to court by the Motion Picture Association of America (MPAA). Torrentspy had pro-actively disabled the logging of any data on its visitors, so that if compelled to, it would be unable to provide any information identifying its users. The company had also inserted clear language in its privacy policy to inform its users that it would not monitor their activity without their consent.[103]

In May of 2007, the MPAA convinced a federal judge to force TorrentSpy to enable logging on its servers – that is, to modify the code running on its servers in order to capture IP address information on its visitors. The judge relied upon the fact that the IP address information is available in computer memory, if just for a few seconds, as evidence that the information is "stored" and thus the company could be compelled to store it.[104]

Demonstrating a level of *chutzpah* common amongst those in the BitTorrent business,[105] TorrentSpy thumbed its nose at the judge's order, and simply blocked all US visitors from accessing the site,[106] citing an "uncertain legal climate in the US regarding user privacy and an apparent tension between US and European Union privacy laws."[107]

E. Hushmail

Since 1999, Hush Communcations, a Canadian technology company, has offered users a free Web-based encrypted email service. [108] In contrast to the free email solutions provided by Microsoft's Hotmail and Yahoo, Hush's Communication's Hushmail product enables users to compose, transmit and receive encrypted email using an encryption key only known to the user. By using this service, a user can securely communicate with another Hushmail user, or one of the hundreds of thousands of existing users of OpenPGP compatible encryption tools.

---

respond with such services to the electronic signal sent over the line. The result was that the Company could no longer supply any of the various services it had promised its customer, including assurance of response in an emergency."

[103] "TorrentSpy.com will not collect any personal information about you except when you specifically and knowingly provide such information." See: TorrentSpy Privacy policy, available at: http://web.archive.org/web/20070410082408/http://www.torrentspy.com/privacy.asp

[104] See generally: http://arstechnica.com/tech-policy/news/2007/08/judge-torrentspy-must-preserve-data-in-ram.ars

[105] See generally various mocking emails in response to DMCA takedowns, http://thepiratebay.org/legal

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

[107] See: http://web.archive.org/web/20070831074431/http://www.torrentspy.com/US_Privacy.asp

[108] Hushmail's free service has a limit of 2MB storage per account, and offers a premium pay service with much higher storage capacity.

While Hushmail's own marketing materials promised users absolute privacy,[109] a drug-related court case proved otherwise. In 2007, Hush received an order from the Supreme Court of British Columbia, which was itself in response to a Mutual Legal Assistance Treaty request by the US Drug Enforcement Agency (DEA). US Court documents reveal that Hush provided the plain-text contents of three users' email accounts to DEA agents.[110]

At the time, Hushmail offered two different forms of encrypted webmail. In the default mode, the user would type her encryption password into a Web form, that would be transmitted to Hush's servers, which would in turn decrypt the email, and then transmit the plaintext of the email to the user. A second more secure solution provided users with a Java-based applet, which downloaded the encrypted mail from Hush's servers, and then decrypted the emails locally. This latter approach provided significantly more security, since the password would never leave the user's computer, and the decrypted emails would never touch Hush' servers or be transmitted over the Internet.

In this particular case, media reports indicate that the suspects were using the more lightweight of the two solutions, in which a user's password was transmitted to and temporarily stored on Hush's servers for the process of mail decryption.[111] Pursuant to the court order, Hush modified their product to capture the passwords of the three suspects, which it then used to decrypt the 12 CDs worth of email that it provided to US law enforcement agents.[112]

While the Java-based solution would have protected users against this particular form of government compelled encryption circumvention, it is not full proof. Just as the company could be compelled to modify the programs that ran on its own servers, it could just as easily be compelled to create a modified version of its Java tool which would steal the user's password.[113] Once news of Hush's compliance with the court order became public, Phil Zimmerman, the original designer of Pretty Good Privacy (PGP) and a member of Hush Communication's Advisory Board defended the company, telling one journalist that:

> "If your threat model includes the government coming in with all of force of the government and compelling service provider to do things it wants them to do, then there are ways to obtain the plaintext of an email. Just

---

[109] The company's website stated that "not even a Hushmail employee with access to our servers can read your encrypted e-mail, since each message is uniquely encoded before it leaves your computer." See: http://www.wired.com/threatlevel/2007/11/encrypted-e-mai

[110] See: http://www.wired.com/images_blogs/threatlevel/files/steroids.source.prod_affiliate.25.pdf

[111] "The rub of that option is that Hushmail has — even if only for a brief moment — a copy of your passphrase. As they disclose in the technical comparison of the two options, this means that an attacker with access to Hushmail's servers can get at the passphrase and thus all of the messages." See: http://www.wired.com/threatlevel/2007/11/encrypted-e-mai

"The only way to decrypt encrypted Hushmail messages stored on our servers is with the private keys associated with the senders and recipients of those messages, and the only way to access those private keys is with the associated passphrases. …. The key point, though, is that in the non-Java configuration, private key and passphrase operations are performed on the server- side. This requires that users place a higher level of trust in our servers as a trade off for the better usability they get from not having to install Java and load an applet." Email from Hush CEO Brian Smith to Wired News Reporter Kevin Poulsen: http://blog.wired.com/27bstroke6/hushmail-privacy.html

[112] "In the case of the alleged steroid dealer, the feds seemed to compel Hushmail to exploit this hole, store the suspects' secret passphrase or decryption key, decrypt their messages and hand them over." See: http://www.wired.com/threatlevel/2007/11/encrypted-e-mai

[113] "Smith concurs and hints that Hushmail's Java architecture doesn't technically prohibit the company from being able to turn over unscrambled emails to cops with court orders … **The extra security given by the Java applet is not particularly relevant, in the practical sense, if an individual account is targeted.**"

because encryption is involved, that doesn't give you a talisman against a prosecutor. They can compel a service provider to cooperate …. It would be suicidal for [Hush's] business model if they [ignored court orders] …. there are certain kinds of attacks that are beyond the scope of their abilities to thwart. They are not a sovereign state."

F. The Java Anonymous Proxy

While all of the preceding examples relate to the Government gaining access to or circumventing the privacy protections in commercial services, it appears that legal coercion can similarly be used to sneak backdoors into Open Source software products.

There are now several open source software projects which aim to provide end-users with the ability to anonymously browse the Internet. While Tor is perhaps the most well known of these, others do exist, including the Java Anonymous Proxy (JAP), a software system designed by researchers from several German universities. Each system is designed differently, but in general, they all provide users with privacy by bouncing their encrypted Internet traffic through several servers around the world. Ideally, a government watching a suspect's network connection will not be able to learn which Web sites she is visiting, while the owners of those Web sites will not be able to identify the true IP address of the anonymous visitor.

In mid 2003, the JAP network went down "due to a hardware failure." When the service was restored, users were informed that they had to install an "upgraded version" of the application in order to again use the anonymizing network. No explanation was given for the necessary upgrade. However, since JAP was an open source project, users could look through the source code and quickly determine which lines of code in had been added to the latest version. Savvy users quickly discovered a few suspicious looking lines of source code:

"CAMsg::printMsg(LOG_INFO,"Loading Crime Detection Data....\n");"

"CAMsg::printMsg(LOG_CRIT,"Crime detected - ID: %u - Content: \n%s\n",id,crimeBuff,payLen);"

When confronted by members of the security community, the JAP developers acknowledged the existence of the "crime detection function" in the system, and revealed that it had been inserted there in response to a court order sought by the German Federal Office of Criminal Investigation. They pledged that privacy in the JAP system was safe, because only "one Web site [was] currently being disclosed, and only under court-ordered monitoring."[114]

This revelation resulted in a significant amount of criticism from members of the academic security community, as well as multiple negative articles in the press. While the JAP developers were merely complying with the court's

---

[114] "Except for the case mentioned above, the protection of the users' anonymity is and will remain the central warranty of AN.ON. The AN.ON operators warn against the generalisation of this single case and the general jeopardising of the whole service. Anonymity in the internet makes still sense when the access to a single website with illegal content is recorded for a limited time period due to a court decision." See: https://www.datenschutzzentrum.de/material/themen/presse/anonip_e.htm ,

See also: http://www.theregister.co.uk/2003/08/21/net_anonymity_service_backdoored/.

order, they still suffered significant damage to their project's reputation. According to a statement by the developers in 2006, only one court order has ever been issued forcing them to use the backdoor.[115]

V. The law

While these examples clearly demonstrate that governments have forced service providers to insert back doors into their own products, the legal justification requiring the company to comply is not always clear. Often, the public only learn of the company's assistance to the government through a brief mention in court documents. However, the legal documents presented to the company are rarely if ever made public. There are several laws which can be used to justify the compelled insertion of back doors in products. These areas of US law will now be highlighted.

A. The Wiretap Act (Title III)

The Wiretap Act regulates the collection of actual content of wire and electronic communications. Codified in 18 U.S.C. §§ 2510-2522, the Wiretap Act was first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and is generally known as "Title III". Prior to the 1986 amendment by Title I of the ECPA, it covered only wire and oral communications. Title I of the ECPA extended that coverage to electronic communications.[116]

18 U.S.C. §§ 2518(4) states that:

> An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person **shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception** unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted.

18 U.S.C. §§ 2518(4) also states that:

> 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.

In the in-car navigation case discussed earlier in this paper, the court determined that the term "other person" in 18 U.S.C. §§ 2518(4) also included "an individual or entity who both provides some sort of service to the target of the surveillance and is uniquely situated to assist in intercepting communications through its facilities or technical abilities." At least based on this case, and the court's ruling of the Wiretap Act, the law can be used to justify forcing a service provider to create new functionality in its products solely for the purpose of wiretapping customers.

---

[115] "In 2006, there has been only one single surveillance court order to single Mix operators. A few exactly specified web addresses were affected. The observation has been stopped after the court order expired (one month). " See: http://anon.inf.tu-dresden.de/strafverfolgung/index_en.html

[116] http://ilt.eff.org/index.php/Privacy:_Wiretap_Act

While the details of the government's Magic Lantern/CIPAV system have yet to be revealed, some legal experts did discuss the possible means through which the government might be able to compel anti-virus vendors to ignore or even white list the FBI's spyware tool. An attorney with the Electronic Frontier Foundation told one journalist that "The government would be pushing the boundaries of the law if it attempted to obtain such an order … There's simply no precedent for this sort of thing." He did point to the Wiretap Act as one possible avenue for this coercion, adding that "There is some breadth in that language that is of concern and that the Justice Department may attempt to exploit."[117]

B. *United States v. New York Telephone Co. (1977)*

One of the most relevant cases relating to this issue is that of *United States v. New York Telephone Co.* In this case, based upon a showing of probable cause, the District Court authorized the FBI to install and use pen register surveillance devices[118] on two telephones used by the suspects of a government investigation. The court also directed the telephone company to furnish the FBI "all information, facilities and technical assistance" necessary to install and use the devices. The telephone company refused to lease to the FBI phone lines that were needed for unobtrusive installation of the pen registers, and thereafter asked the court to vacate that portion of the pen register order directing respondent to furnish facilities and technical assistance to the FBI on the ground that such a directive could be issued only in connection with a Title III wiretap order.

The Court of Appeals held that the District Court abused its discretion in ordering the telephone company to assist in installing and operating the pen registers, and expressed concern that such a requirement could establish an undesirable precedent for the authority of federal courts to impress unwilling aid on private third parties.

The Supreme Court was far more willing to extend these coercive powers to the US government, looking primarily to the All Writs Act. That Act states that:

> "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[119]

With regard to this case, first, the court noted that "[t]he assistance of the Company was required … to implement a pen register order which … the District Court was empowered to issue." It also noted that "without the Company's assistance there is no conceivable way in which the surveillance authorized by the District Court could have been successfully accomplished … The provision of a leased line by the Company was essential to the fulfillment of the purpose -- to learn the identities of those connected with the gambling operation -- for which the pen register order had been issued.

Then, citing the All Writs Act, the court stated that "[u]nless appropriately confined by Congress, a federal court may avail itself of all auxiliary writs as aids in the performance of its duties, when the use of such historic aids is calculated in its sound judgment to achieve the ends of justice entrusted to it."[120] Furthermore, "The power conferred by the

---

[117] http://news.cnet.com/Will-security-firms-detect-police-spyware---page-2/2100-7348_3-6197020-2.html

[118] Pen register devices record the numbers dialed by a phone, without overhearing oral communications or indicating whether calls are completed.

[119] 28 U.S.C. § 1651(a).

[120] *Adams v. United States ex rel. McCann*, 317 U. S. 269, 317 U. S. 273 (1942).

[All Writs] Act extends, under appropriate circumstances, to persons who (though not parties to the original action or engaged in wrongdoing) are in a position to frustrate the implementation of a court order or the proper administration of justice. Here respondent … was not so far removed as a third party from the underlying controversy that its assistance could not permissibly be compelled by the order of the court based on a probable cause showing that respondent's facilities were being illegally used on a continuing basis."

Concluding, the court wrote that "[t]he conviction that private citizens have a duty to provide assistance to law enforcement officials when it is required is by no means foreign to our traditions."[121] However, in an effort to place at least some limit to this power, court stressed that the order "required minimal effort on the part of the Company and *no disruption to its operations.*"

C. Other mentions of the All Writs Act

While *New York Telephone* is the most important case relying on the All Writs Act, this is not the only time that the Government has depended upon this age-old statute.

In a 2005 case related to attempts by the government to obtain the real time location information of mobile phone customers, the Department of Justice revealed that:

> Currently, the government routinely applies for and upon a showing of relevance to an ongoing investigation receives "hotwatch" orders issued pursuant to the All Writs Act. Such orders direct a credit card issuer to disclose to law enforcement each subsequent credit card transaction effected by a subject of investigation immediately after the issuer records that transaction.
>
> While the evidence sought by All Writs orders in such cases is often pre-existing, see, e.g., United States v. Doe, 537 F. Supp. at 839 (ordering disclosure of 6 prior months of telephone toll records), there is no legal impediment to issuing such an order for records yet to be created. See, e.g., In re Application of the U.S.A. For An Order Directing X To Provide Access to Videotapes, 2003 WL 22053105, No. 03-89 (Aug. 22, 2003 D. Md.) (directing that production of subsequently-created videotapes made by security camera installed in apartment hallway).[122]

In the same case, noted that the power to issue supplemental orders in aid of the court's jurisdiction "extends to persons who are not defendants and have not obstructed justice."[123] Again, for this authority, the government pointed to the All Writs Act:

> [A]ny additional authority needed for the Court to direct prospective disclosure of cellsite information, the Court already possesses it under the All Writs Act … which authorizes the issuance of orders in aid of the Court's jurisdiction.

The Judge in this case disagreed with the Department of Justice, denying their request, and stating that:

> The government thus asks me to read into the All Writs Act an empowerment of the judiciary to grant the executive branch authority to use investigative techniques either explicitly denied it by the legislative branch,

---

[121] 434 U.S. at 175 n. 24, 98 S.Ct. 364.

[122] See: http://www.eff.org/legal/cases/USA_v_PenRegister/celltracking_govt_reply.pdf

[123] United States v. Doe, 537 F. Supp. 838 (E.D.N.Y. 1982)

> or at a minimum omitted from a far-reaching and detailed statutory scheme that has received the legislature's intensive and repeated consideration. Such a broad reading of the statute invites an exercise of judicial activism that is breathtaking in its scope and fundamentally inconsistent with my understanding of the extent of my authority.[124]

The government's attempt to turn the All Writs Act into the All Surveillance Act appears to have been frustrated, at least in this case. [125] However, it appears that its argument has been repeatedly (and successfully) used to justify the issuance of credit card "hotwatch" orders.

D. The Foreign Intelligence Surveillance Act (FISA)

While both the Wiretap Act and the All Writs Act generally apply to court orders sought by law enforcement agencies, there is one other legal avenue through which the government can force service providers to insert backdoors. However, instead of applying to the FBI, the powers provided by the Foreign Intelligence Surveillance Act are generally used by the National Security Agency. The 2008 Protect America Act amended FISA to state that:

> The Director of National Intelligence and Attorney General may direct a person to …. immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition in such a manner as will protect the secrecy of the acquisition and produce a minimum of interference with the services that such person is providing to the target … The Government shall compensate, at the prevailing rate, a person for providing information, facilities, or assistance pursuant to subsection (e).

While details on the government's interpretation and use of this law are understandably absent, some commentators have argued that the law gives "the government wide powers to order communication service providers such as cell phone companies and ISPs to make their networks available to government eavesdroppers."[126]

VI. Encryption can be circumvented

Let us now go back to our earlier hypothetical world in which all cloud services have switched to data encryption with a key private to the user. In this situation, the government would not be able to use a subpoena to force the revelation of a user's private files, since the service provider would only possess encrypted data. However, it might very well be possible for the government to force that company to place a backdoor in its Web based product in order to steal the user's key. That is, when the user entered her key in the Google Docs product, instead of keeping the key in local memory, a copy of it could be silently transmitted to a FBI server.

While market forces might be able to provide a solution to the problem of the third party doctrine by encouraging the use of encryption, there are no market forces or technology that can protect a company from a lawful order compelling that company to backdoor its own product.

A. Traditional software is pretty hard to back door

---

[124] http://www.eff.org/deeplinks/2005/10/all-writs-redux

[125] http://www.eff.org/deeplinks/2005/10/all-surveillance-act

[126] http://www.wired.com/threatlevel/2007/08/analysis-new-la

One of the defining features of the Internet era is the ability of technology firms to later fix problems in their products, to release new features after the date of initial sale, and in some cases, to even remove useful features.[127] A fix that would in years past have required a costly and slow product recall can now be deployed to all customers with a mere software update. This ability to release products half-finished, rushing them to the market confident in the knowledge that remaining issues can be fixed with a later patch has led to a situation that some experts call a state of perpetual beta.

In some cases, these updates must be manually installed by the user. When this is the case, adoption rates can be extremely low – even if update is downloaded automatically, and the user is notified that an update is available. This poses a problem to government agencies that might wish to compel a traditional software company, such as an operating system vendor, into creating and deploying a back door. If users cannot be convinced to download and install critical security updates that might protect them from hackers, how can they be convinced to download government back doors that may attempt to access their private files.

Another problem associated with the insertion of back doors in traditional software products is the fact that most vendors do not know their customers identities. Many copies of Microsoft Windows and other software suites are bundled with new computers, or negotiated as part of site licenses for companies and universities. Unless the user registers their software purchase, the software supplier simply will not know which individual is associated with any one serial number. The widespread problem of software piracy makes this even worse, since these users are even less likely to register their illicit installations under their own names.

This gap between an identifiable customer and a software installation poses a serious barrier to the government's ability to compel most traditional software providers into rolling out covert back doors, even if the customer can be convinced to install it. Sure, the company could opt to supply to the sneaky update to *all* customers based on the assumption that the government's suspect will be one of the impacted users. However, this approach is likely to draw the attention of security researchers who routinely reverse engineer software updates in order to learn which flaws have been fixed.

The move to cloud computing makes it far easier for the government to effectively force the deployment of covert back doors. This is due to a few key features inherent in the Web 2.0 application model: identifiable customers, automatic, silent updates and the complete absence of visible product releases.

---

[127] "A federal court in Marshall, Texas, ordered EchoStar Communications, the second-largest satellite TV operator in the United States, to disable the digital video recorders currently being used by millions of its customers. EchoStar, which has more than 12 million customers, has been ordered to disable the DVRs within 30 days." See: http://www.redherring.com/Home/18034

"Apple is clamping down on piracy by imposing restrictions on the way that music can be shared via the iTunes service. Changes to the service stop people listening across the internet to playlists of songs created by others." See: http://news.bbc.co.uk/2/hi/technology/2946180.stm

"In iTunes 4.5, you can authorize up to five Macs or Windows computers to play your purchased music -- up from three. But Apple giveth and Apple taketh away: you can now burn a playlist containing purchased music up to seven times (down from ten). And the old workaround of simply changing the playlist slightly does not work." See: http://lawgeek.typepad.com/lawgeek/2004/04/meet_the_new_it.html

"However, Apple has moved to restrict the streaming capability. In the good old days it used to support five simultaneous listeners, but now allows only allows five listeners a day." See: http://www.theinquirer.net/inquirer/news/156/1002156/apple-squeezes-itunes-customers

B. Updates and the cloud

One of the most useful features of the Web 2.0 paradigm, for both provider and customer, is that users are always running the latest version of a particular Web based application. There is simply no need to coax an update, because it is simply impossible to run anything *but* the latest version.

The vast majority of cloud based software runs in a Web browser. In this model, a user visits a Web page, and her browser immediately downloads the programmatic code which is used to implement the Web page's functionality. When the user re visits that same Web site the next day, her Web browser again requests the same content, and downloads it from the Web server.[128] If the Web site owner has updated the code, that new version of the page will be downloaded, without any notification to the user that the code running on her computer today is different than the day before.

Traditional software vendors, both application and operating system, ship software with a version number. Users can, if they know how, find out which version of Microsoft Word, Photoshop or Quicken they are running. In fact, many applications display their current version number when starting.

Contrast this to the situation for the users of cloud based services. Google does not provide a version number for its Gmail or Docs service. Neither does Yahoo, Facebook, or MySpace. New features might be announced, or suddenly appear, however, when bugs are fixed, these are usually done so quietly with no notification to the user.

If a Google Docs starts up her computer, connects to the Internet and accesses her documents, she has no way of knowing if her browser is executing different code than it ran the day before. The same user running Firefox or Microsoft Windows would have a much better chance of knowing this, and in most cases, of declining to perform an update if one was made available.

Finally, most cloud providers know a significant amount more about their customers than traditional software companies. Unless a customer has given a false name, email providers and social networking companies know who their customers are as well as the names and contact information for their friends. As a result, if law enforcement agencies serve a subpoena in order to obtain the files for a specific customer, most cloud computing providers know exactly which account to target.

This shift in the effectiveness of software updates and the ease of customer identification significantly weakens the ability of cloud providers to protect their customers' privacy with encryption. That is, while Google could add encryption to its Docs application, the company could be just as easily be forced to add a back door in to the browser code which would steal the user's key. As we have just explained, this would be automatically downloaded and executed the next time that the user logged in, with no way for her to avoid the update, or even know that it was applied.

VII. Conclusion

[128] In some cases, a cloud application might cache a local copy of its JavaScript code in the user's browser (such as with Gmail). However, this is only done for performance reasons – if the user clears his or her cache, uses a new computer, or if the application provider releases a new version of their software, the JavaScript code will be re-obtained. Likewise, there is no notification to the user that a cached copy is being used, or a new copy is being downloaded.

As this paper has noted, the mass adoption of cloud computing based services has significantly tipped the scales of privacy away from the end user – it is now much easier for hackers, private investigators or law enforcement and intelligence agents to access a user's private files. Furthermore, the government can now leverage economies of scale, and take advantage of the fact that the user no longer needs to be consulted or notified before her data is seized. In many cases, due simply to the reality that a single company is responsible for storing private data for millions of users, the government can obtain data on an additional individual at almost no cost. That is, the cost of adding one more person to the subpoena is free.

While the ease of government access made possible by the third party doctrine is certainly troubling, the use of data encryption and strict adherence to no-logging policies can act as a significant balance against this power. Were the third party doctrine to be done away with, the threats of hackers breaking into a company's servers and insiders peeking at a user's files would still remain – encryption is a technique that provides protection against all of these threats.

As we have documented at length, the real threat to end-user privacy is the ease with which the government can force an application provider to insert a backdoor or flaw in its own products. While this is certainly a risk that existed pre-cloud computing, it has been made more effective, and more difficult to discover through the shift to software as a service. Simply put, the government can order a change, and the next day, every user of a service specified in the government's order will be running code with that backdoor – a level of adoption that was never possible before.

Given the number of different laws which can be used to force service providers to violate their own customers' privacy, it is unlikely that Congress would agree to any form of legislative fix which took away this power. Thus, we focus our attention upon transparency related legislation as well as technology based solutions to this problem.

A. Improving transparency through user education

B. Privacy through open source software

Of all of the other examples given earlier in this paper, most came to light through their mention in court documents. Furthermore, while we know that *a* manufacturer of GPS navigation equipment was forced to snoop on its customers, six years on, we still do not know the identity of the company.

The *Java Anonymous Proxy* incident highlighted earlier in this paper also stands out because it is the one instance in which users themselves discovered the back door. Simply put, it is exceedingly difficult to covertly install a backdoor into an open-source product, as inquisitive users will look through the changes in the code, and notice the new feature. Furthermore, due to the highly distributed nature of many open source projects, even if developers in one country are forced into secrecy by a gag order, developers in another will not be. These developers will already be highly familiar with the source code, and thus will be most likely to notice and publicize any suspect changes.

Applying this observation to the market for cloud computing services, we argue that while the government could *in theory* force the Mozilla Corporation to a backdoor into its Weave encrypted browser add-on, such an action would likely soon be discovered. Whereas a court order could effectively lead to the circumvention of an encrypted cloud computing service provided by Google, Yahoo and Microsoft, we do not believe that the government's coercive powers are effective against open source software. Simply put, when users entrust their private data to companies using proprietary software, even when those companies provide users with the ability to encrypt data with a private key, those users are still vulnerable to government ordered back doors. While these risks still apply to the users of open source tools, this risk is significantly reduced.

To slightly paraphrase Linus Torvalds, the creator of the Linux operating system, given enough eyeballs, all surveillance bugs are shallow.[129]

This is not to say that the cloud computing model is fundamentally insecure, or that users should avoid all of Google's services. We merely argue that if companies do opt to deploy cloud services with strong data encryption, that the programmatic code which has access to the user's password be open source software – preferably the Web browser. As an example, Firefox could provide a simple Application Programming Interface (API) through which cloud computing services could request the encryption and decryption of files – with Firefox itself handling the user's password and all encryption functionality. This would provide the best of both worlds: privacy of user's most important data, while permitting private companies to offer innovative technology which they did not wish to share with their competitors.

[129] http://en.wikipedia.org/wiki/Linus%27s_Law