Before the
Federal Trade Commission
Washington, D.C.

"Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

COMMENT OF CHRISTOPHER SOGHOIAN[1]

February 18, 2011

Consumers reasonably expect that companies will protect their private data. As such, warrantless, voluntary disclosures of user data to law enforcement agencies should not be considered a "commonly accepted practice." Companies should be required to obtain informed consent from their customers before making such disclosures.

Consumers expect that third parties to whom they entrust their data will protect their privacy

Long before the creation of the Internet, consumers entrusted their private data to third parties. The courts recognized that these individuals still maintain a reasonable expectation of privacy over their communications. This applies to letters sent through the postal system,[2] phone calls,[3] and more recently, email.[4]

Building on this baseline expectation of privacy, consumers have several other reasons to expect that companies will protect their privacy.

---

1. Graduate Fellow, Center for Applied Cybersecurity Research, and Ph.D. Candidate, School of Informatics and Computing, Indiana University. Email: chris@soghoian.net
2. See *United States v. Jacobsen*, 466 U.S. 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy").
3. See *Katz v. United States*, 389 U.S. 352 (1967) (the caller was "surely entitled to assume that the words he utter[ed] into the mouthpiece w[ould] not be broadcast to the world.") and at 351, ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.")
4. *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) (holding that "[t]he privacy interests in [mail and email] are identical"). *United States v. Warshak* ---F.3d ----, 2010 WL 5071766 (6th Cir. Dec.14, 2010 ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection.") and ("email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve.")

First, as multiple surveys have documented and the FTC has acknowledged,[5] when consumers see the words "privacy policy" on a website, they believe that the site will protect their privacy.[6] This has a rather significant impact, as practically every commercial website has a prominently posted privacy policy.[7]

Second, many companies, particularly those offering communications services and applications repeatedly promise to protect their customers' privacy, both in statements on their websites and in quotes to the press. For example:

> "Verizon has a longstanding and vigorous commitment to protecting its customers' privacy and takes comprehensive steps to protect that privacy."[8]

> "At Verizon, privacy is a key priority. We know that consumers will use the full capabilities of our communications networks only if they trust that their information will remain private."[9]

> "At Google, we are keenly aware of the trust our users place in us, and our responsibility to protect their privacy."[10]

> "Google values our users' privacy first and foremost. Trust is the basis of everything we do, so we want you to be familiar and comfortable with the integrity and care we give your personal data."[11]

> "Microsoft takes customers' privacy seriously . . . ."[12]

---

5. Robert Mullens, Is that coupon worth the risk to your personal privacy?, Network World, http://www.networkworld.com/community/node/71037, "The FTC's [Laura] Berger said consumers mistakenly believe that if a company posts a privacy policy on its Web site that this means that the consumer's private data won't be shared"

6. Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathaniel Good, and Jens Grossklags. "The FTC and Consumer Privacy in the Coming Decade" Federal Trade Commission. Washington, DC. Nov. 2006. http://works.bepress.com/chris_hoofnagle/4/ ("Most fundamentally, research indicates that a large majority of American adults believe that a "privacy policy" on a website indicates some level of substantive privacy protection for their personal information. The finding is not an aberration. Two major national surveys two years apart (in 2003 and 2005) revealed virtually the same percentage of Americans—almost 60%-- believing that "when a website has a privacy policy, that means it will not share information about them with other websites or companies." In the 2005 survey, where the statement was presented in true/false form, 59% incorrectly said the statement was true and an additional 16% said they didn't know if it were true or false.")

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

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

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

10. Privacy FAQs, Google, http://www.google.com/privacy_faq.html (last visited Sept. 26, 2010).

11. Marissa Mayer, What comes next in this series? 13, 33, 53, 61, 37, 28…, Official Google Blog (July 3, 2008, 1:36 PM), http://googleblog.blogspot.com/2008/07/what-comes-next-in-this-series-13-33-53.html.

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

> "At Microsoft, we believe individuals should control the use of their personal information online, and should be free from fear that their personal and financial data will be stolen or used by others without their consent."[13]

It is difficult to imagine why an average consumer, after navigating the websites of these firms, reading news articles that include such statements, or browsing Google's Privacy YouTube channel (which includes 49 videos that explain the lengths the company takes to protect the privacy of its customers),[14] would not take these firms at their word and reasonably expect these companies to protect their data.

Lawful disclosures of user data to law enforcement agencies

Under US law there are two ways that law enforcement agencies can obtain private user data from communications and computing service providers: compelled disclosure and voluntary disclosure. The rules governing these two forms of disclosure differ, as do the options available to companies that might wish to put their users' privacy first.

In response to a valid legal demand (for example, a subpoena, an order issued under 18 U.S.C. § 2730(d), or probable cause warrant issued under Rule 41 of the Federal Rules of Criminal Procedure), companies **are required** to provide the information sought to the respective law enforcement agency).

However, this is not the case for voluntary disclosures by service providers. 18 U.S.C. § 2702(b)(8) and 18 U.S.C. § 2702(c)(4) permit the disclosure of communications content and non-content:[15] "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[16]

As the U.S. Internet Service Provider Association notes, "There is never an 'emergency' obligation on an ISP to disclose."[17] If a provider refuses to disclose its customers' data, the government can always obtain a subpoena, a 2703(d) order, or a search warrant, and compel the company to disclose the information. As such, a company's policy on emergency requests is one of the most useful indicators for its overall commitment to user privacy, as it is one of the few times a company can put its customers' privacy first and say no.

Unfortunately, because the law does not require service providers to tell their customers when their data has been voluntarily disclosed to the government, the likelihood that consumers ever learn of disclosures is extremely low. Furthermore, few companies will publicly discuss the extent to which they receive emergency requests, and federal reporting requirements for such requests are largely worthless.

---

13. Microsoft and Privacy, Microsoft (Sep. 2009), http://go.microsoft.com/?linkid=9688090
14. http://www.youtube.com/user/googleprivacy
15. 18 U.S.C. §§ 2702(b)(8), 2702(c)(4) (2006).
16. 18 U.S.C. § 2702(b)(8) (2006).
17. U.S. Internet Serv. Provider Ass'n, Electronic Evidence Compliance — A Guide for Internet Service Providers, 18 Berkeley Tech. L.J. 945, 962 (2003).

Even so, it is clear that the practice is widespread. For example, of the 88,000 lawful requests and demands Verizon received from federal, state and local officials in 2006, 25,000 were requests for emergency assistance, and as such, received no prior judicial review.[18] Verizon has not released any statistics detailing how many of these 25,000 emergency requests it refused to comply with.

Small print in privacy policies regarding voluntary disclosures are insufficient

As the FTC made quite clear in its settlement with *Sears Holding*,[19] disclosures in the small print of a privacy policy are not sufficient if clear statements promising more have been made to consumers. In the Sears Holding case, the company represented to consumers that its software would track their "online browsing," but it was only in the End User License Agreement that the firm acknowledged that the software might also capture "confidential personally identifiable information such as UserID, password, credit card numbers, and account numbers." As the FTC noted in its complaint, "these facts would be material to consumers in deciding to install the software. Sears Holding's failure to disclose these facts, in light of the representations made, was, and is, a deceptive practice."

Google, Facebook, Microsoft, and Verizon all acknowledge in their respective privacy policies that they may voluntarily disclose their customers' data to law enforcement agencies.[20] However, as FTC Chairman Leibowitz has acknowledged, "[w]e all agree that consumers don't read privacy policies – or

---

18. Letter from Randal S. Milch, Sr. Vice Pres., Verizon Bus., to John D. Dingell, Edward J. Markey & Bart Stupak, U.S. Reps (Oct. 12, 2007), available at http://markey.house.gov/docs/telecomm/Verizon_wiretaping_response_101207.pdf at 5.

19. In the Matter of Sears Holdings Management Corporation, a corporation. FTC File No. 082 3099.

[20] See: Google Privacy Policy, http://www.google.com/privacy/privacy-policy.html, ("Google only shares personal information with other companies or individuals outside of Google in the following limited circumstances … We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to … protect against harm to the … safety of … its users or the public as required or permitted by law."),
Microsoft Online Privacy Statement, http://privacy.microsoft.com/en-us/fullnotice.mspx,
("We may access or disclose information about you, including the content of your communications, in order to: (a) comply with the law or respond to lawful requests or legal process; (b) protect the rights or property of Microsoft or our customers, including the enforcement of our agreements or policies governing your use of the services; or (c) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of Microsoft employees, customers or the public."),
Facebook Privacy Policy, http://www.facebook.com/policy.php, ("To respond to legal requests and prevent harm. We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law. This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction, and are consistent with generally accepted international standards. We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities."),
Verizon Privacy Policy, http://www22.verizon.com/about/privacy/policy/#outsideVz, ('We may disclose information that individually identifies our customers in certain circumstances, such as: to comply with valid legal process including subpoenas, court orders or search warrants, and as otherwise authorized by law; in cases involving danger of death or serious physical injury to any person or other emergencies;").

EULAs, for that matter."[21] Given that these firms have all made bold promises to protect their customers' privacy, these weasel words in their respective privacy policies do relieve them of the obligation to stand by their prior public commitments.

The FTC's proposed commonly accepted practices

The preliminary FTC staff privacy report "identified a limited set of 'commonly accepted practices' for which companies should not be required to seek consent once the consumer elects to use the product or service in question." One of these "commonly accepted practices" was:

> **Legal compliance and public purpose**: Search engines, mobile applications, and pawn shops share their customer data with law enforcement agencies in response to subpoenas. A business reports a consumer's delinquent account to a credit bureau.

Describing the motivation for this specific item, the report states that "[o]ther [practices], including the use of consumer data exclusively for fraud prevention, legal compliance, or internal operations, are sufficiently accepted – or necessary for public policy reasons – that companies do not need to request consent for them."

The report does not provide sufficient detail to determine if the "commonly accepted" disclosures are only those required by law or, if the FTC staff also believes that voluntary disclosures should be considered to be "commonly accepted."

Voluntary disclosures should not be considered a "commonly accepted" practice as they are contrary to consumers' reasonable expectation of privacy, as well as the repeated public statements by companies regarding their commitment to protecting user privacy.

Companies should of course be free to voluntarily disclosure their customers' data to law enforcement agencies when the law permits. However, they should have to seek informed consent from their customers before doing so. Furthermore, they should not be permitted to disclose user data voluntarily while simultaneously sending clear, yet deceptive signals to consumers about the degree to which they will protect their privacy.

Quite simply, if companies are going to publicly tout their commitment to privacy, they must honor those statements.

Respectfully submitted,

/s

Christopher Soghoian

---

21. FTC Chairman Jon Leibowitz, Introductory Remarks, FTC Privacy Roundtable, December 7, 2009, available at : http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf