COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

TO

THE FEDERAL TRADE COMMISSION

Bureau of Consumer Protection
A Preliminary FTC Staff Report on
"Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

February 18, 2011

The Federal Trade Commission (FTC) has requested comments on a December 2010 staff report, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," [Hereinafter "FTC Report" or "Report"].[1] According to the FTC, the report is the culmination of a series of roundtables "to determine how best to protect consumer privacy while supporting beneficial uses of information and technological innovation."[2] In brief, the FTC Report recommends the establishment of a Do Not Track mechanism, the adoption of "privacy by design" techniques, and the use of simplified privacy notices.[3]

Pursuant to the FTC Notice, the Electronic Privacy Information Center (EPIC) submits these comments to address the issues raised in the FTC Report and to set out recommendations that would better safeguard the privacy interests of consumer. EPIC is

[1] Federal Trade Commission, Consumer Protection Bureau, "Protecting consumer Privacy in an Era of rapid Change; A proposed Framework for Businesses and Policymakers," Notice and Request for Comments, December 2010, *available at* https://ftcpublic.commentworks.com/ftc/consumerprivacyreport/.
[2] Federal Trade Commission, Consumer Protection Bureau, "Protecting consumer Privacy in an Era of rapid Change; A proposed Framework for Businesses and Policymakers," *available at* http://ftc.gov/os/2010/12/101201privacyreport.pdf [hereinafter *Report*].
[3] *Id.*

a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in protecting individuals' privacy on the Internet, and has played a leading role in developing the authority of the FTC to address emerging privacy issues. [4]

In summary, EPIC supports meaningful efforts to strengthen privacy protection for consumers and Internet users. EPIC believes that the FTC can continue to protect consumers through Section 5 enforcement against unfair and deceptive practices as it has in the past. EPIC also supports the implementation and enforcement of Fair Information Practices. EPIC also supports the deployment of Privacy Enhancing Techniques ("PETs", also described as "Privacy by Design.")[5] And EPIC supports the creation of an independent US privacy agency.

The FTC report addresses these goals in part, but mistakenly endorses self-regulation and "notice and choice," and fails to explain why it has not used its current Section 5 authority to better safeguard the interests of consumers.

Comments and Recommendations

1. *The FTC Should Pursue Meaningful Investigations and Enforce Section 5 Fully*

[4] See Letter from EPIC Executive Director Marc Rotenberg to FTC Commissioner Christine Varney (Dec. 14, 1995), available at http://epic.org/privacy/internet/ftc/ftc_letter.html. *See generally* EPIC: Federal Trade Commission, http://epic.org/privacy/internet/ftc; EPIC: Online Tracking and Behavioral Profiling, http://epic.org/privacy/consumer/online_tracking_and_behavioral.html; EPIC: Children's' Online Privacy Protection Act (COPPA), http://epic.org/privacy/kids/; EPIC: Choicepoint, http://epic.org/privacy/choicepoint/; EPIC: Cloud Computing, http://epic.org/privacy/cloudcomputing/; EPIC: Social Networking Privacy, http://epic.org/privacy/socialnet/.

[5] *See* Herbert Burkert, *Privacy Enhancing Technologies: Typology, Critique, Vision* in PHIL AGRE & MARC ROTENBERG, TECHNOLOGY AND PRIVACY: THE NEWS LANDSCAPE 125 (MIT Press 1998).

Outside of sectoral statutory authority, the FTC's primary enforcement authority for consumer privacy is derived from 15 U.S.C. § 45, commonly known as "section 5" of the Federal Trade Commission Act (FTCA). Section 5 of the FTCA allows the FTC to investigate "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." This provision provides a legal basis for the FTC to investigate business activities that threaten consumer privacy, to pursue complaints, to issues reports, and to enforce orders. In the Report, the Commission states that "Commission staff will also continue to use its authority under Section 5 of the FTC Act, and other statutes it enforces, to investigate privacy or data security practices that may violate such laws." However, the Commission fails to explain why it has failed to use this authority in pending complaints involving privacy issues of greatest concern to Internet users.

In the past, the FTC has used Section 5 authority effectively to address emerging challenges to consumer privacy. For example, in 2001, EPIC, along with a coalition of groups, initiated a complaint to the FTC regarding Microsoft Passport.[6] The complaint detailed the risks to privacy and security of a single Internet authentication scheme, and set out a broad range of recommendations.

Following the receipt of the complaint from EPIC and the other consumer organizations, the Commission undertook an extensive investigation and subsequently required Microsoft to implement a comprehensive information security program for Passport and similar services.[7] The FTC's action led the company to develop a new

[6] EPIC FTC Complaint, In the Matter of Microsoft Corporation, July 26, 2001, *available at* http://epic.org/privacy/consumer/MS_complaint.pdf.
[7] *In the Matter of Microsoft Corporation*, File No. 012 3240, Docket No. C-4069 (Aug. 2002), *available at* http://www.ftc.gov/os/caselist/0123240/0123240.shtm. *See also* Fed. Trade Comm'n, "Microsoft Settles

model for online authentication that protected privacy and security. Because of decisive action by the FTC on a critical Internet issue, innovation and competition followed.

Relying again on the FTC's Section 5 authority, in 2004 EPIC filed a complaint with the Commission regarding databroker Choicepoint, Inc.[8] The complaint set out numerous risks to consumer privacy resulting from the business practices of the company. In that matter, the Commission again undertook an extensive investigation and subsequently determined that ChoicePoint's failure to employ reasonable security policies compromised the sensitive personal data of consumers, and assessed fines of $15 million,[9] leading to significant reforms across the industry.

Additionally, the FTC used its Section 5 authority to settle a case against LifeLock, a company that used false claims to sell identity protection services to consumers.[10] LifeLock agreed to pay $11 million to the Commission and $1 million to a group of State Attorney Generals, and must take stronger steps to protect consumer information and refrain from making any deceptive statements.

Yet in recent years, the Commission has failed to use its Section 5 authority in some of the most important consumer privacy issues of the day. Even after the problems have been well documented, the Commission has refused to take meaningful action to

---

FTC Charges Alleging False Security and Privacy Promises" (Aug. 2002) ("The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years."), *available at* http://www.ftc.gov/opa/2002/08/microst.shtm.

[8] EPIC FTC Complaint, In the Matter of Choicepoint, Dec. 16, 2004, *available at* http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[9] Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties*, $5 Million for Consumer Redress, Jan. 26, 2006, *available at* http://www.ftc.gov/opa/2006/01/choicepoint.shtm.

[10] FTC, "LifeLock will pay 12 million to settle charges by the FTC and 35 states that identity protection and data security claims were false," Mar. 9, 2010, *available at* http://www.ftc.gov/opa/2010/03/lifelock.shtm.

protect consumers, reflecting a lack of leadership and technical understanding in areas of increasing interest to American consumers. The following comments will highlight examples of major privacy violations that the FTC has failed to take action on, resulting in harm to American consumers.

A. Google Cloud Computing

In March 2009, EPIC filed a complaint with the FTC regarding Google's Cloud Computing services.[11] The complaint addressed one of the most pressing issues facing Internet users in recent years – the risks that might result from the transfer of personal information and applications on the personal computer or laptop of an end-user to a service provided by a company on a remote server, no longer under the control of the user.

In the complaint, EPIC petitioned the Commission to open an investigation to determine the adequacy of the privacy and security safeguards, to assess the representations made by Google, the leading firm offering these services, to determine whether the firm has engaged in unfair and/or deceptive trade practices, and to take any such measures as are necessary, including to enjoin Google from offering such services until safeguards are verifiably established.[12] EPIC stated that such action by the Commission is necessary to ensure the safety and security of information submitted to Google by American consumers, American businesses, and American federal agencies.[13]

The public has expressed similar concerns about the privacy implications of cloud computing. According to a Pew Internet & American Life Project report, 69% of

[11] EPIC FTC Complaint, In re Google and Cloud Computing Services, Mar. 17, 2009, *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.
[12] *Id.*
[13] *Id.*

Americans are making use of "cloud computing," allowing their data to reside in online servers accessible via the Internet.[14] In an October 2009 study conducted by Penn, Schoen & Berland Associates, 87% of respondents were still not familiar with how cloud computing worked, yet 85% responded they would be concerned about the security of information stored in a "cloud," or online server.[15]

In February 2009, the World Privacy Forum (WPF) published a report on the risks to privacy and confidentiality from cloud computing.[16] Robert Gellman, who prepared the report, found "a user's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud provider."[17] Further, "for some types of information and some categories of cloud computing users, privacy and confidentiality rights, obligations, and status may change when a user discloses information to a cloud provider."[18]

One of the privacy implications of cloud computing noted in the WPF report is that the transfer of otherwise personal information to cloud providers creates new opportunities for information to be accessed by the government without notice to users.[19] For users, "the loss of notice of a government demand for data is a significant reduction in rights."[20] Another concern is the security of user information: "security requirements for information may also create problems because of the inability of the user to assess the

[14] John Horrigan, pew Internet & American Life Project, *Use of Cloud computing Applications and Services* (September 2008), *available at* http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf.
[15] Penn, Schoen & Berland Associates, *Online Exposure, Offline Uncertainty: Privacy and Security in a Virtual World* (October 2009).
[16] Robert Gellman, World Privacy Forum, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing* (February 2009), *available at* http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.
[17] *Id.* at 6.
[18] *Id.*
[19] *Id.* at 11.
[20] *Id.*

provider's security, to audit security for compliance, or to determine whether the level of security meets statutory or regulatory security requirements."[21]

These concerns over cloud computing were realized when Google experienced a security breach, in which "Google disclosed user-generated documents saved on its Google Docs Cloud Computing Service to users of the service who lacked permission to view the files.[22] There were also three other similar breaches involving Google cloud computing services,[23] all causing harm to consumers. Google's inadequate security was an unfair business practice and a deceptive trade practice because Google had made misrepresentations concerning the security of users' information.[24] A letter by thirty-eight computer researchers and academicians to Google CEO Eric Schmidt raised similar concerns.[25]

Since then, consumers have become increasingly dependent on cloud computing services. According to a recent PEW Internet and Elon University study, most technology experts believe that the next decade will bring increased reliance on internet-based application and Cloud Computing.[26] The survey found that the Cloud Computing brings considerable privacy and security risks.[27] Consumers are increasingly subject to new business practices and shifting privacy policies that leave essential questions about the security and privacy of personal information stored on remote servers unanswered. Not

---

[21] *Id.* at 22.
[22] EPIC FTC Complaint, In re Google, Mar. 17, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.
[23] *Id.*
[24] *Id.*
[25] Jacob Appelbaum, et al., Letter to Google CEO Eric Schmidt re: Ensuring Adequate Security in Google's Cloud based Services (June 16, 2009), *available at* http://files.cloudprivacy.net/google-letter-final.pdf.
[26] Elon University – Pew Internet Survey, "The Future of the Internet, June 11, 2010, *available at* http://www.elon.edu/docs/eweb/predictions/expertsurveys/2010survey/PIP_Future_of_internet_2010_cloud.pdf.
[27] *Id.*

surprisingly, public officials with expertise in privacy matters are examining these services more closely to assess their impact on privacy and security.[28]

But to the extent that the FTC has shown an interest in this topic, it has largely been to discourage investigations by other agencies. The FTC indicated in a comment to the FCC that it was pursuing an investigation on Cloud Computing services but the scope and purpose of the investigation remain unclear.[29]

In the end, the FTC failed to act on one of the most pressing issues facing Internet users.

B. The FTC Has Failed to Protect Consumers from Facebook's Unfair and Deceptive Practices

Facebook is one of the largest Internet firms. Its business practices have an enormous impact on Internet users both in the United States and around the world.[30] EPIC has filed three complaints with the FTC over the past two years concerning significant changes to the privacy rights of Facebook users set out in the Terms of Service and the privacy settings of Facebook users. In December 2009, EPIC, along with a coalition of other groups, filed a complaint with the Commission that focused on Facebook's practice of sharing user information with the public and with third-party application developers.[31] Facebook forced users to convert what had previously been

[28] *See* ENISA, *Cloud Computing: Benefits, Risks, and Recommendations for Information Security* (November 2009), *available at* http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.
[29] FTC Comments on FCC NBP Public Notice #21, Dec. 9, 2009, available at http://fjallfoss.fcc.gov/ecfs/document/view?id=7020352132.
[30] Facebook, *Statistics*, http://www.facebook.com/press/info.php?statistics (last visited Dec. 14, 2009).
[31] EPIC FTC Complaint, In the Matter of Facebook, Inc., Dec. 17, 2009, *available at* http://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

protected under privacy settings into "links," which are "publicly available" information, and users were not given a choice to opt-out of this process.[32] These changes contradicted earlier assurances made by the company that users would be able to protect their information, and contradicted users' reasonable expectations about their privacy.[33] EPIC's complaint also highlighted Facebook's unfair and deceptive social plug-in program, the changes Facebook made to its data retention rules without ever gaining users' consent, and its lack of transparency regarding its use of cookies.[34]

EPIC filed a supplemental complaint in January 2010, when Facebook announced another round of changes which required mandatory disclosure of profile information that had previously been protected by users' privacy settings, including names, profile pictures, and friends lists. [35]

In May 2010, EPIC again asked the FTC to open an investigation into Facebook's unfair and deceptive trade practices. The EPIC complaint states that changes to user profile information and the disclosure of user data to third parties without consent "violate user expectations, diminish user privacy, and contradict Facebook's own representations."[36] The complaint also cites widespread opposition from Facebook users, Senators, bloggers, and news organizations.[37] In the complaint, EPIC asks the FTC to open an investigation into Facebook, to compel Facebook to allow users to choose whether to link and publicly disclose personal information, to compel Facebook to restore

[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] EPIC FTC Supplemental Complaint, In the Matter of Facebook, Inc., January 14, 2010, *available at* http://epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf.
[36] EPIC FTC Complaint, In the Matter of Facebook II, May 5, 2010, *available at* http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf.
[37] *Id.*

its previous requirement that developers retain user information for no more than 24 hours, and to compel Facebook to make its data collection practices clearer and more comprehensible.[38]

Congress also criticized Facebook's actions and urged investigations into their practices. In October 2010, Congressmen Ed Markey (D-MA) and Joe Barton (R-TX) sent a letter to Facebook about the news that Facebook's business partners transmitted personal user data to advertising and Internet tracking companies in violation of the company's policy. In June 2010, the head of the House Judiciary Committee, Rep. Conyers, asked Google Inc. and Facebook to cooperate with government inquiries into privacy practices at both companies.[39] Rep. Conyers asked Facebook to provide a detailed explanation regarding its collection and sharing of user information.[40] In April 2010, Senator Schumer (D-NY) asked the FTC to establish guidelines for social networking sites after Facebook announced it would disclose user data to websites without consent.[41]

Privacy and consumer protection officials in other countries have been active in responding to Facebook's privacy violations. The Canadian Privacy Commission has pursued several investigations of Facebook's privacy controls and has required the company to increase user privacy.[42] And very recently, Facebook was required by

---

[38] *Id.*

[39] "Congressman Seeks Answers from Facebook and Google on Privacy Issues, Congressman John Conyers, Jr., May 28, 2010, *available at* http://judiciary.house.gov/news/100528.html.

[40] Letter from Congressman John Conyers to Google CEO Eric Schmidt, May 28, 2010, *available at* http://judiciary.house.gov/hearings/pdf/Conyers-Google100528.pdf.

[41] "Schumer: Decision by Facebook to Share Users' Private Information with Third-Party Websites Raises Major Privacy Concerns; Calls on FTC To Put in Place Guidelines for Use of Private Information and Prohibit Access Without User Permission, April 26, 2010, *available at* http://schumer.senate.gov/record.cfm?id=324175&.

[42] Facebook Blog, *Improving User Privacy on Platform* (Aug. 27, 2009),

German privacy officials to let users in Germany better hide their e-mail contacts from unwanted ads and solicitations.[43]

Facebook continues to make disturbing changes to its privacy settings. In August 2010, Facebook introduced "Places," which makes user location data routinely available to others, including Facebook business partners, regardless of whether users wish to disclose their location.[44] There is no single opt-out to avoid location tracking; users must change several different privacy settings to restore their privacy status quo. And finally, in January 2011, Facebook announced a plan to allow third party access to users' home addresses and personal phone numbers.[45] After much criticism, Facebook temporarily suspended the plan, but said it will go forward once it has made further changes.[46]

In the face of all this information, however, the FTC has not take any action against Facebook in response to any privacy complaint. It is a remarkable abdication of consumer protection authority, possibly unparalleled in the history of the Federal Trade Commission.

Of the original EPIC complaint to the FTC concerning Facebook, FTC Consumer Protection Bureau Director David Vladeck wrote that the complaint "raises issues of particular interest."[47] Yet, the Commission has taken no further action. Moreover, the

---

http://developers.facebook.com/news.php?blog=1&story=292 (acknowledging that it made changes to improve user privacy as "a result of our work with the Office of the Privacy Commissioner of Canada, which ahs spent more than a year reviewing our privacy policies.").

[43] Kevin J. O'Brien, "Facebook Makes Deal with German Privacy Group, The New York Times, January 24, 2011, *available at* http://www.nytimes.com/2011/01/25/technology/25facebook.html?ref=technology.

[44] *See* Facebook Places, http://www.facebook.com/places/.

[45] Facebook Developer Blog, "Platform Updates: new User Object Fields, Edge.remove Event and more," January 14, 2011, *available at* http://developers.facebook.com/blog/post/446.

[46] Facebook Developer Blog, "Improvements to Permissions for Address and Mobile Number, January 18, 2011, *available at* http://developers.facebook.com/blog/post/447.

[47] Letter from David Vladeck, Director of FTC Consumer Protection Bureau, to Marc Rotenberg, EPIC President, January 14, 2010, *available at* http://epic.org/privacy/inrefacebook/Facebook_Vladeck_Letter.pdf.

FTC failed to respond to consumer concerns widely expressed about Facebook, and failed to make use of its current Section 5 authority. One can only wonder how the Commission treats complaints that do not raise "issues of particular interest."

C. Google Buzz

In February 2010, EPIC filed a complaint with the FTC regarding Google Buzz.[48] Buzz was Google's attempt to transform its popular e-mail service into an untested social networking service.[49] As a consequence, Google displayed social networking lists based on a user's most frequent address book contacts, without user permission. The activation of Buzz not only disclosed users' contact lists, but more specifically disclosed the contacts with whom users communicate most often.[50] The change was widely criticized.[51] EPIC's complaint cited clear harms to service subscribers, and alleged that the change in business practices "violated user expectations, diminished user privacy, contradicted Gogole's privacy policy, and may have violated federal wiretap laws." EPIC filed a supplemental complaint in March that elaborated on the specific ways in which Google Buzz constituted a violation of Google's stated Privacy Policy for Gmail.[52]

Ten Members of Congress also asked the FTC to investigate Google Buzz, citing the EPIC complaint, and expressing concern about "the unintended dangers that this alleged privacy breach poses for children" and "Google's practice of automatically using consumers' email address books to create contact lists for Buzz and then publicly

---

[48] EPIC FTC Complaint, In the Matter of Google Inc., February 2010, *available at* http://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf.
[49] Google Buzz, http://www.google.com/buzz.
[50] EPIC FTC Complaint, In the Matter of Google, Inc.
[51] *See Id.*
[52] EPIC FTC Supplemental Complaint, In the Matter of Google, Inc., March 2010, *available at* http://epic.org/privacy/ftc/googlebuzz/Google_Buzz_Supp_Complaint.pdf.

disclosing the names of these private contacts by posing the information online."[53] The letter lists potential harms resulting from Google Buzz's deceptive practices, including the revealing of journalists' confidential sources or the disclosure of information about a consumer's medical history or political views.[54]

The FTC did nothing about Google Buzz. In a letter, Bureau of Consumer Protection Director David Vladeck stated that EPIC's complaint "raises interesting issues that relate to consumer expectations about the collection and use of their data."[55] Further, the Director highlighted the importance of having consumers "understand how their data will be used" and allowing consumers the "opportunity to exercise meaningful control over such uses."[56]

Yet, the FTC failed to take any meaningful action against the invasive privacy violations of Google Buzz that caused real harm to consumers. The FTC failed to respond to consumer concerns about Google Buzz, and failed to make use of its current Section 5 authority.

D. Google Street View – WiFi Data Collection

In an attempt to get the attention of a federal agency that might actually be interested in safeguarding American consumers, in May 2010 EPIC wrote to the Federal Communications Commission (FCC), urging the FCC to open an investigation into the consumer data Google Street View cars were collecting from WiFi hotspots.[57] In its letter, EPIC stated that Google routinely and secretly intercepted and stored user

[53] Letter from House Members to Chairman Leibowitz, March 25, 2010, *available at* http://epic.org/privacy/ftc/googlebuzz/3_26_10_FTC_Letter_re_Google_Buzz.pdf.
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] EPIC letter to Federal Communications Commission, May 18, 2010, *available at* http://epic.org/redirect/111910EPIC-FCC.html.

communications data.[58] EPIC said that this conduct appears to violate federal wiretap laws as well as the US Communications Act.[59] The FCC responded. In June 2010 the Wall Street Journal confirmed that the FCC was investigating Google Street View's WiFi data collection, following the complaint from EPIC.[60]

It became clear in the months following EPIC's letter that Google had been purposefully and secretively collecting WiFi data in thirty countries over a three-year period through its Street View vehicles, which Google originally maintained merely collected images.[61] Google only admitted to collecting the WiFi data after European investigations revealed it.[62] Google further admitted that in addition to the MAC addresses and SSIDs it said it was collecting, it also collected payload data – including full e-mails, passwords, and URLs.[63]

In May 2010, Members of Congress asked the FTC to investigate Google's secretive collection of WiFi data, perhaps thinking that the FTC would do something.[64] In the letter, the Representatives asked the FTC whether Google's actions "form the basis of an unfair or deceptive act or practice that constitutes harm to consumers" and whether

---

[58] *Id.*
[59] *Id.*
[60] Amy Schatz and Amir Efrati, "FCC Investigating Google Data Collection," The Wall Street Journal, November 11, 2010, *available at* http://online.wsj.com/article/SB10001424052748704804504575606831614327598.html?mod=WSJ_hp_LEFTWhatsNewsCollection.
[61] *See Id.*
[62] See Google Blog Post (April 27, 2010) http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html; see also updates (may 17, 2010 and June 9, 2010) http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html
[63] Google Blog, "WiFi Data Collection: An Update," *available at* http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.
[64] Reps. Markey and Barton letter to FTCc Chairman Leibowitz, May 19, 2010, *available at* http://republicans.energycommerce.house.gov/Media/file/News/051910_Markey_Barton_to_FTC_Google_WiFi.pdf.

Google's actions are "illegal under federal law."[65] No response by the FTC to this letter can be found on the Congressmen's website. In addition, unlike the FCC, the Federal Trade Commission never pursued an independent investigation of Street View, examined the data collected by Google in the United States, or even acknowledged the findings of other agencies.

Many US states and foreign countries have investigated Google, and several have found that Google violated national privacy laws. The Spanish Data Protection Agency filed suit against Google Street View for five violations of Spanish law.[66] Canada's Privacy Commissioner determined that Google violated Canadian privacy law when the company's Street View cars collected user information from wireless networks.[67] British officials announced that Google violated UK data protection laws as well.[68] In lieu of a fine, Google UK will undergo an audit and must sign a commitment to ensure that data protection breaches do not happen again. The New Zealand Privacy Commissioner found that Google violated New Zealand law.[69] Connecticut Attorney General, and Senator-elect, Richard Blumenthal issued a "civil investigative demand," similar to a subpoena, for access to the data Google's Street View cars collected from homes and businesses in

[65] *Id.*
[66] Spanish Data Protection Agency, "The Spanish DPA opens Enforcement Proceedings to Google for the Collection of Personal data from Wi-Fi Networks fro Street View," October 18, 2010, *available at* http://epic.org/privacy/streetview/documents/101018_GOOGLE_WI-FI.pdf.
[67] Office of the Privacy Commissioner of Canada, "Google Contravened Canadian Privacy Law, Investigation Finds," October 19, 2010, *available at* http://www.priv.gc.ca/media/nr-c/2010/nr-c_101019_e.cfm.
[68] UK Information Commissioner's Office, "Information Commissioner Announces Outcome of Google Street View Investigation, November 3, 2010, *available at* http://www.ico.gov.uk/~/media/documents/pressreleases/2010/google_inc_street_view_press_release_0311.2010.pdf.
[69] New Zealand Privacy Commissioner, "Google Agrees to Protect Privacy Better, December 14, 2010, *available at* http://privacy.org.nz/media-release-google-agrees-to-protect-privacy-better/.

Connecticut.[70] "Google's story changed," Blumenthal has said, "first claiming only fragments were collected, then acknowledging entire emails."

But the federal government agency charged with protecting American consumers has done nothing. The FTC recently announced in a letter to Google that the Commission was ending its "investigation" into Google's collection of WiFi data through its Street View cars.[71] In a letter to Google's law firm, David Vladeck, director of the Bureau of Consumer Protection at the FTC, explained that while he has "concerns" about Google's "internal review process," the agency is satisfied by steps Google has taken and "assurances" Google has made to the agency.[72]

The FTC has failed to respond to consumer concerns about Google Street View's WiFi data collection, and has failed to make use of its current Section 5 authority.

E. Echometrix

Finally, it is worth noting that EPIC brought the practices of Echometrix to the attention of the Federal Trade Commission. Echometrix was the company that was offering "Parental control" software while simultaneously collecting data from children for marketing purposes.[73] The practice was unfair and deceptive on its face. But the FTC dilly-dallied. However, the Department of Defense moved effectively to address consumer privacy concerns. Upon learning of the EPIC complaint, it prohibited the subsequent distribution to military families. The Army and Air Force Exchange Service pulled My Military Sentry, which collects data for marketing purposes, from its online

[70] CT Attorney General's Office, "Attorney General Demands Access to Data Improperly Collected in CT by Google Street View Cars," December 10, 2010, *available at* http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=469804.
[71] Letter from David Vladeck, FTC, to Albert Gidari, Perkins and Cole, October 27, 2010, *available at* http://www.ftc.gov/os/closings/101027googleletter.pdf.
[72] *Id.*
[73] See "EPIC: Echometrix," http://epic.org/privacy/echometrix/.

store: "The collection of AAFES customer information (personal or otherwise) for any other purpose than to provide quality customer service is prohibited . . . . Giving our customers the ability to opt out does not address this issue."[74]

The New York attorney general also took action against Echometrix. Under the settlement with the New York Attorney General's Office, Echometrix will pay a $100,000 penalty to the state of New York, and has agreed not to "analyze or share with third parties any private communications, information, or online activity to which they have access."[75]

More than a year after EPIC filed the complaint, after the product was pulled by the Department of Defense, and after the NY Attorney General had obtained civil damages, the FTC announced a settlement in which Echometrix agreed not to share any data and to destroy the information it had collected in its marketing database, but was not required to pay any fines.[76]

2. *Comprehensive Federal Privacy Laws should be based on Fair Information Practices*

The FTC Report continues to place misguided emphasis on the "notice and choice" model.[77] The Report discusses a simpler version of notice and choice, but that model does not work because privacy notices are not stable or meaningful.[78] There is not a fixed

---

[74] *Id.*

[75] Office of the New York Attorney General, "Cumo Announces Agreement Stopping Software Company 'Echometrix' from Selling Children's Private Online Conversations to Marketers," (Sept. 15, 2010), available at http://www.ag.ny.gov/media_center/2010/sep/sep15a_10.html.

[76] Federal Trade Commission, "FTC Settles with Company that Failed to Tell Parents that Children's Information Would be Disclosed to Marketers," Nov. 30, 2010, available at http://www.ftc.gov/opa/2010/11/echometrix.shtm.

[77] *See* Report, *supra* note 2 at 52-63

[78] *See* Testimony of EPIC President Marc Rotenberg on "An Examination of the Google-Doubleclick Merger and the Online Advertising Industry: What are the Risks for Competition and Privacy?" before the Subcommittee on Antitrust, Competition Policy and Consumer Rights, Committee on the Judiciary,

metric as there are with food labels or MPG labels that allow consumers to make meaningful choices. The closest experiment with brief privacy notices to date is the recent experience with the Facebook privacy settings. And the failure of the Commission to act on behalf of consumers when Facebook changed these settings makes clear the utter pointlessness of this approach to privacy protection

In order to be effective, privacy protection must be based on the implementation and enforcement of Fair Information Practices. And these are not "Principles," e.g. "FIPPS," they are the actual "practices" that businesses are expected to adopt and enforce.[79] The Fair Information Practices that form the basis of such legislation should be modeled on the Privacy Act of 1974[80] and on the Organization for Economic Co-operation and Development (OECD) Privacy Guidelines[81]. The guidelines set out by the OECD include: data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[82] The principles outlined in the Privacy Act are very similar:

> (1) Permit an individual to determine what records pertaining to him are collected, maintained used or disseminated by such agencies;
>
> (2) Permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

United States Senate, Sept. 27, 2007, available at http://judiciary.senate.gov/hearings/testimony.cfm?id=2955&wit_id=6686.

[79] The recent popularization of the phrase "Fair Information Practices Principles" waters down one of the key insights of the 1973 report: that effective privacy protection focuses on what organizations actually do, not what they claim to do.

[80] Privacy Act of 1974, 5 USC § 552a.

[81] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[82] *Id.*

(3) Permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) Collect, maintain, use or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) Permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) Be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.[83]

But the Privacy Act only applies to the collection of information by federal agencies in the U.S., not to the collection of information by private companies or non-governmental entities. In these areas, the U.S. followed a policy of sectoral regulation in the 1980s and early 1990s, but then adopted the approach of self-regulation for Internet-based commerce.[84]

The same principles outlined in the Privacy Act should form the basis of

[83] Privacy Act of 1974, 5 USC § 552a.
[84] Anita L. Allen, *Privacy Law and Society,* Thomson Reuters, 2011 ("United States policy-makers have favored a combination of multiple, limited-purpose public laws and industry self-regulation…over the years, Congress has enacted numerous privacy-protection statutes, resulting in a patchwork quilt of special-purpose rules.").

comprehensive federal privacy legislation that will protect all citizens' privacy in the face of invasive online tracking and behavioral profiling. In Europe, many countries have passed national laws based on FIPs that apply to both the public and private sector.[85] It is time for the U.S. to follow that example.

3. *Creation of an Independent Privacy Authority Will Improve Privacy Protections*

The FTC Report does not even contemplate the idea of an office devoted entirely to protecting consumer privacy, but it is clear now that the FTC lacks the competence and the will to address the privacy challenges faced by consumers. The creation of an independent privacy agency will enhance privacy protections for consumers. Such an entity would have the authority and the expertise to ensure that agencies are complying with the Privacy Act and to help agencies anticipate new challenges involving rapidly changing technology and privacy issues. The organization should be independent of the executive branch. The correct model would be an independent agency.

In 1973 the Department of Health, Education and Welfare established a special panel to study privacy issues arising from the growing use of automated date processing equipment.[86] That report led to the development and passage of the Privacy Act of 1974.[87] But that report also made clear that the cornerstone of an effective federal policy is a permanent privacy agency.[88] Virtually every study that has looked at the US experience since 1974 has concluded that the United States needs an independent privacy

[85] Robert Gellman, "Fair Information Practices: A Basic History," May 13, 2010, *available at bobgellman.com/rg-docs/rg-FIPShistory.pdf.*
[86] US Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens*, (July 1973), *available at* http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm.
[87] 5 U.S.C. § 552a (1974).
[88] HEW Report, *supra* note 5.

agency.[89] In countries across the world, independent privacy agencies have been established to address similar concerns. The European Union has implemented extensive privacy directives that establish legal rights for all citizens in the European Union countries. Non-EU countries, from Canada[90] to Hong Kong,[91] are pursuing comprehensive privacy agendas led by privacy agencies. These government agencies routinely report on the handling of privacy complaints,[92] the emergence of new privacy issues, and proposed measures to protect privacy. These reports help the public and the government understand the status of privacy protections in their country and develop new approaches to replace old ones.

But there is still no privacy agency in the United States. In fact, President Obama is only just beginning *now* to nominate people to staff the Privacy and Civil Liberties Oversight Board.[93] In many respects, this is surprising. It is clear that the absence of a privacy agency in the federal government remains a critical problem. Having announced

---

[89] *See, e.g.,* Jeffrey Rosen, "Nude Breach: Why Privacy Always Loses," The New Republic, December 13, 2010 (Compared to their European counterparts, U.S. privacy offices lack both independence and regulatory teeth…the Government needs a genuinely independent institution dedicated to protecting Americans' privacy); Bob Gellman, "*A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board,"* 54 HSTLJ 1183,1208, April 2003 ("Only an independent [privacy] agency can criticize the policies and practices of the executive branch…it is undisputed that many routine government functions can have drastic effects on the privacy rights and interests of individuals."); David H. Flaherty, *Protecting Privacy in Surveillance Societies* 22, 381 (1989) ("…it is not enough simply to pass a data protection law . . . an agency charged with implementation is essential to make the law work in practice. . . A statute by itself is an insufficient countervailing force to the ideological and political pressures for efficiency and monitoring of the population that are at work in Western society."); Marc Rotenberg, *In support of a Data Protection Board in the United States*, 8 Government Information Quarterly 79-93 (1991) ("A privacy protection commission was a key component of the original privacy protection scheme developed by the Congress in the early 1970s but was never enacted. Recent public polling data suggests that the creation of a similar board today would be supported by a wide majority of Americans.").

[90] Office of the Privacy Commissioner of Canada, Mandate and Mission of the OPC, http://www.privcom.gc.ca/aboutUs/index_e.asp.

[91] Office of the Privacy Commissioner for Personal Data, Hong Kong, Homepage, http://www.pcpd.org.hk/.

[92] Office of the Privacy Commissioner of Canada, http://www.privcom.gc.ca/i_i/index_e.asp.

[93] The White House, Nominations sent to Senate, December 17, 2010, *available at* http://www.whitehouse.gov/the-press-office/2010/12/17/nominations-sent-senate.

numerous programs that hinge on the collection and dissemination of Americans' personal information, some institutional balance must be established to ensure that these proposals receive adequate review. This would be a small investment in what many Americans consider their number one concern about our nation's infrastructure – the protection of personal privacy.

Conclusion

In numerous examples, the FTC has failed to use its current authority to protect the privacy interests of American consumers and Internet users. Considering all of the attention that the FTC has devoted to the privacy issue, it is remarkable that the Commission does not have more to show for its efforts. And the FTC's continuing support for self-regulation and short privacy notices is both ill-informed and out of date. Been there. Done that.

To safeguard the interests of American consumers and Internet users, it is necessary to create a new agency with the technical competence and political will to protect privacy.

Marc Rotenberg
EPIC Executive Director

Sharon Goott Nissim
EPIC Consumer Privacy Fellow

February 18, 2011