COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

TO

THE FEDERAL TRADE COMMISSION

In the Matter of Google, Inc.

FTC File No. 102 3136

May 2, 2011

The Federal Trade Commission ("FTC") has requested public comments on a Proposed Consent Order with Google.[1] The consent agreement in this matter would settle "alleged violations of federal law prohibiting unfair or deceptive acts or practices."[2] The Consent Order follows from the FTC's Complaint, which alleges that "Google violated Section 5(a) of the FTC Act by falsely representing to users signing up for Gmail that it would use their information only for the purpose of providing them with Web-based email."[3] The Complaint also alleges that Google "falsely represented to consumers that it would seek their consent before using their information for a purpose other than that for which it was collected."[4] The FTC Complaint further alleges that "Google deceived consumers about their ability to decline enrollment in certain features of Buzz. In addition, the Complaint alleges that Google failed to disclose adequately that certain information would become public by default through the Buzz product."[5]

---

[1] FTC, *Google, Inc.; Analysis of Proposed Consent Oorder to Aid Public Comment,* File No. 102-3136, 76 Fed. Reg. 18762 (Apr. 5, 2011), *available at* http://www.ftc.gov/os/caselist/1023136/110405googlebuzzfrn.pdf;
[2] *Id.*
[3] *Id.* at 18763.
[4] *Id.*
[5] *Id.*

Finally, the FTC complaint alleges that Google "misrepresented its compliance with the U.S.-EU Safe Harbor Framework, a mechanism by which U.S. companies may transfer data from the European Union to the United States consistent with European law."[6]

These comments on the FTC's proposed Consent Order are submitted on behalf of the Electronic Privacy Information Center ("EPIC"), a public interest research center in Washington, D.C. EPIC was 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 consumer privacy, and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[7] EPIC brought the Google Buzz matter to the attention of the FTC, and now provides these comments and recommendations to ensure that meaningful protection of consumer privacy results from this proceeding.[8]

Section I sets out the procedural history of the investigation concerning the business practices that gave rise to this Consent Order. Section II sets out EPIC's involvement and expertise in this matter. Sections III and IV detail the FTC Complaint and summarize the FTC Consent Order. Section V sets out EPIC's comments and

---

[6] *Id.*

[7] *See, e.g.,* Letter from EPIC Executive Director Marc Rotenberg to FTC Commissioner Christine Varney, EPIC (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry) *available at* http://epic.org/privacy/internet/ftc/ftc_letter.html; EPIC, *In the Matter of DoubleClick, Complaint and Request for Injunction, Request for Investigation and for Other Relief*, before the Federal Trade Commission (Feb. 10, 2000), available at http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; EPIC, *In the Matter of* Microsoft *Corporation, Complaint and Request for Injunction, Request for Investigation and for Other Relief,* before the Federal Trade Commission (July 26, 2001), available at http://epic.org/privacy/consumer/MS_complaint.pdf; EPIC, *In the Matter of Choicepoint, Request for Investigation and for Other Relief,* before the Federal Trade Commission (Dec. 16, 2004), *available at* http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[8] *See generally* EPIC, *In re Google Buzz: Concerning the Privacy of Electronic Address Books,* available at http://epic.org/privacy/ftc/googlebuzz/default.html.

recommendations regarding Part III of the Consent Order, concerning Google's Comprehensive Privacy Policy, that would strengthen consumer protections and enhance the Agreement's effectiveness.

In summary, EPIC supports the findings in the FTC Complaint and the directives contained in the Consent Order. The Complaint makes clear that companies should not engage in unfair and deceptive trade practices, particularly in the collection and use of personal data. In such circumstances, the FTC has the authority and the obligation to act to protect the interests of consumers. The Consent Order that follows from the Complaint outlines several measures to safeguard the interests of consumers.

To further protect the interests of consumers and to make clear the full scope of a Comprehensive Privacy Program that is mandated for Google, EPIC recommends that the FTC require Google to:

- Require Fair Information Practices for all of Google's products and services;
- Build a Do Not Track mechanism into the company's Chrome web browser;
- Encrypt all of its cloud computing services;
- Protect the privacy and anonymity of Google Books users;
- Cease tracking mobile phone users' locations or web-browsing habits without explicit opt-in permission;
- Require a warrant before giving user data to law enforcement;
- Fully delete user search history and other information collected after six months;
- Keep non-Gmail users' emails fully private; and
- End the collection of data transmitted by residential wireless routers.

These obligations are consistent with the current Order and do not require further

revision.

In addition, EPIC recommends that the FTC:

- Make the results of Google's privacy Assessments available to the public; and
- Apply the provisions of its Agreement with Google to all other Internet companies.

EPIC would also like to call the FTC's attention to the many public comments submitted in the course of this proceeding. Several organizations, including the Association of Research Libraries and the Center for Digital Democracy, submitted substantial comments regarding further steps that the Federal Trade Commission should take. Comments were submitted directly to the FTC. EPIC also facilitated the submission of comments to the agency, and established a public petition in support of a strong Comprehensive Privacy Program for Google and other Internet companies.

I. PROCEDURAL HISTORY

On February 9, 2010, Google chose to make the personal information of Gmail subscribers widely available to others without their knowledge or consent.[9]

On February 16, 2010, EPIC filed a complaint with the Federal Trade Commission, urging the Commission to investigate Google Buzz.[10]

On February 26, 2010, the Commission sent a letter to EPIC in response to EPIC's complaint.[11] In the letter, the FTC Bureau of Consumer Protection Director stated that the EPIC "complaint raises a number of privacy concerns relating to Google's use of consumers' personal information in launching Buzz."[12] The FTC Consumer Protection Director said further, "We appreciate your valuable participation in our public roundtables, as well as the specific concerns you raised in your complaint to the Commission."[13]

On March 2, 2010, EPIC supplemented its original complaint to the FTC detailing specific ways in which Google Buzz constituted a violation of Google's stated Privacy Policy for Gmail.[14]

On March 29, 2010, ten Members of the US House of Representatives asked the FTC to investigate Google Buzz, given "Google's practice of automatically using

---

[9] 76 Fed. Reg. at 18763.
[10] EPIC, *In the Matter of Google, Complaint, Request for Investigation, Injunction, and Other Relief,* before the Federal Trade Commission (Feb. 16, 2010) [hereinafter "EPIC Google Complaint"]; *See generally,* EPIC, *In re Google Buzz, available at* http://epic.org/privacy/ftc/googlebuzz/default.html
[11] Letter from David C. Vladeck, FTC Office of the Director, Bureau of Consumer Protection to Marc Rotenberg, Executive Director, Electronic Privacy Information Center (Feb. 26, 2010), *available at* http://epic.org/privacy/ftc/googlebuzz/Vladeck_Letter_GoogleBuzz.pdf.
[12] *Id.*
[13] *Id.*
[14] EPIC, *In the Matter of Google, Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief,* before the Federal Trade Commission (Mar. 2, 2010) [hereinafter "EPIC Google Supplemental Complaint"];

consumers' e-mail address books to create contact lists for Buzz and then publicly disclosing the names of those private contacts" online.[15]

On March 30, 2011, the FTC reached a proposed agreement with Google regarding Buzz and other Google products and services.[16] In the announcement of the proposed Agreement and Consent Order, the FTC noted that "Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched." [17]

II. EPIC's INVOLVEMENT AND EXPERTISE

EPIC's complaint to the FTC regarding Google Buzz described Google's misrepresentations and contradictions concerning several aspects of its Buzz service.[18] EPIC alleged that the company's actions constituted unfair and deceptive practices under Section 5 of the FTC Act.[19] The main findings in EPIC's complaint are detailed below.

[15] *Letter from House Members to FTC* (March 29, 2010), *available at* http://epic.org/privacy/ftc/googlebuzz/3_26_10_FTC_Letter_re_Google_Buzz.pdf.
[16] FTC Proposed Settlement Order with Google, *available at* http://www.ftc.gov/opa/2011/03/google.shtm.
[17] FTC, *FTC Charges Deceptive Privacy Practices in Google's Rollout of its Buzz Social Network,* March 30, 2011, *available at* http://www.ftc.gov/opa/2011/03/google.shtm.
[18] *See* EPIC Google Complaint.
[19] *Id.* at 13-15.

Users Were Automatically Enrolled in Google Buzz

The day that Google launched Google Buzz, Gmail users were met with a screen introducing them to Buzz. Users had the option to click on a button to "Check out Buzz" or "Nah, go to my inbox" instead. Regardless of which button a user clicked, Buzz was activated.[20]

Google Disclosed Users' Email Contacts in Buzz

Once Buzz was activated, the tool automatically populated a user's following lists using that user's most frequent email contacts.[21] Users were not warned that this would happen.[22] In order to participate in Google Buzz one had to make a public profile with one's name and photo. These "following" and "followed by" lists were automatically visible to the public once a user created a public profile.[23] Even contacts without a public profile would appear on a user's public follower list. These "follow" lists specifically disclosed the contacts with whom users communicated most often.[24] Users could click a link to expand their Buzz network by harvesting the personal contact lists of other people

There Was No Clear Way for a User to Opt Out of Buzz or Make Information Non-Public

The only way a user could hide the "follow" lists was by clicking through several links to edit her profile and un-check a box.[25]

Google Buzz Violated Gmail Privacy Policy

---

[20] *Id.* at 4.
[21] *Id.* at 4, 12.
[22] *Id.* at 4.
[23] *Id.* at 5.
[24] *Id.*
[25] *Id.*

Gmail's privacy notice described the collection and use of personal data for the purpose of providing *email* service. The personal information section promised users that the company would only use their contact lists and other related data in order to provide the service, clearly referring to Gmail.[26] Google Buzz used Gmail users' contact lists and related data for a separate and unrelated service, in violation of the Gmail privacy notice.[27] Google Buzz processed Gmail account information and Gmail message information in violation of Google's privacy notice.[28]

Google Buzz Caused Significant Harm to Gmail Users

Google Buzz violated users' expectation of privacy in their emails. It had particularly potentially severe effects on a number of categories of people, including: activists in authoritarian countries, those involved in abusive domestic situations, professionals who promise confidentiality (lawyers, journalists, etc.), children, and those with sensitive medical issues.

EPIC's Recommendations Regarding Google Buzz

EPIC's primary recommendation in its complaint was for the FTC to "enjoin [Google's] unfair and deceptive business practices and require Google to protect the privacy of Gmail users."[29] Specifically, EPIC urged that the FTC:

1. Compel Google to make Google Buzz a fully opt-in service for Gmail users;
2. Compel Google to cease using Gmail users' private address book contacts to compile social networking lists;
3. Compel Google to give Google Buzz users more control over their information, by allowing users to accept or reject followers from the outset;

[26] EPIC Google Supplemental Complaint at 2-3.
[27] *Id.*
[28] *Id.*
[29] EPIC Google Complaint at 15.

4. Provide such other relief as the Commission found necessary and appropriate.[30]

III. FTC COMPLAINT ALLEGATIONS

The FTC's Complaint addressed many of the issues set out in the EPIC filing. The FTC elaborated on the Buzz public profile and the way in which Gmail misrepresented the extent to which users could control their information. Google stated that in using Buzz, users could post to the world or privately to whom they chose. But in order to actually limit who could see the profile and followers, users had to click an "edit" link and then uncheck a box.[31] So if a user did not take extra, burdensome steps to edit her profile, her previously confidential data would be made publicly available by default. [32]

The FTC also found that the default setting for posted items was public, and these were searchable on the Internet and indexed by search engines. Buzz also connected to information that users had on other Google apps such as Picasa and Reader. Gmail user preferences to block email contacts from viewing information about them were not carried over to Buzz. Users could not block followers who did not have a public Google profile. If a Buzz user wanted to reply to someone, Buzz would fill in that person's private email address.[33]

---

[30] *Id.* at 15-16.
[31] FTC Complaint.
[32] FTC Complaint *In The Matter Of* Google Inc., Docket No. 102 3136, at 4, March 30, 2011, *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzcmpt.pdf.
[33] *Id.* at 4-5.

Section 5 Violations

The FTC set out four violations of Section 5 – false and misleading acts by Google that constituted deceptive acts and practices.

First, Google had represented, expressly or by implication, that it would use information from Gmail customers only for email service.[34]

Second, Google had represented that it would get consumers' consent to use information they provided for a different purpose than what it was collected for, but did not get consent before using the Gmail information for Buzz. [35]

Third, Google represented that those who clicked "Nah" and Turn off Buzz" would not be enrolled, but they were instead enrolled in certain features. [36]

Fourth, Google represented through the Buzz screens and statements like "how do you want to appear to others" that consumers would be able to have control over what information was made public through their profile. Google did not disclose, or did not adequately disclose, that frequent contacts would be made public by default and that "user information submitted through other Google products would be automatically broadcast through Buzz." [37]

Safe Harbor Violations

The Safe Harbor is a procedure for US companies to transfer personal data outside the EU while abiding by the requirements of the European Union Data Protection Directive. The Department of Commerce and the European Commission

[34] *Id.* at 5.
[35] *Id.* at 6.
[36] *Id.*
[37] *Id.*

(EC) negotiated the Safe Harbor. Companies must certify that they comply with seven principles and related requirements that meet the EC's adequacy standard.

Google transferred data collected from Gmail users in Europe to the US for processing before launching Buzz. Google said in its privacy policy that it adhered to the US Safe Harbor privacy principles. To comply with Safe Harbor, a company must certify that it complies with seven Safe Harbor principles, including Notice, Choice, Onward Transfer, Access, Security, Data Integrity, and Enforcement.[38]

However, Google did not comply with these principles. Google "did not give Gmail users notice before using the information collected for Gmail for a purpose other than that for which it was originally collected. [Google] also did not give Gmail users choice about using their information for a purpose that was incompatible with the purpose for which it was originally collected."[39] Therefore, Google's representation that it complied with Safe Harbor privacy principles was false and misleading and constituted a deceptive act or practice. [40]

[38] U.S. Department of Commerce, "U.S.-EU Safe Harbor Overview," available at http://www.export.gov/safeharbor/eu/eg_main_018476.asp.
[39] FTC Complaint at 7-8.
[40] *Id.* at 6-7.

IV. FTC PROPOSED AGREEMENT

Part I - Google Barred from Misrepresentations

Part I of the Agreement bars Google from misrepresenting "the protection of privacy and confidentiality of covered information," including but not limited to: the purpose of collection and use of covered information and the extent to which consumers may exercise control over the collection, use, and disclosure of covered information. [41]

Part I also applies to Google's compliance with "any privacy, security, or any other compliance program sponsored by the government or any other entity" including the Safe Harbor provisions. [42]

Part II – Google Barred from Third-Party Sharing

Before any "new or additional sharing" of Google users' information "with any third party"[43] that "(1) is a change from stated sharing practices in effect at the time [Google] collected such information, and (2) results from any change, addition or enhancement to a product or service by respondent," Google shall "clearly and prominently" disclose that the user information will be shared with that third party,

---

[41] FTC Agreement Containing Consent Order *In The Matter Of* Google, Inc., March 30, 2011, Section 1, *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf. (The definition of "covered information" includes information Google collects from or about an individual, including: first and last name, home address, including street name and city, email address, user identifier/screen name, "persistent identifier" such as IP address, phone number including cell, list of contacts, physical location, or any other information combined with the above about or from a consumer. *Id.* at "Definitions," #5.)

[42] *Id.* at Section 1.

[43] "Third party" is defined as any individual or entity *other than* (1)Google or (2) service provider of Google that uses or gets covered information for Google and at its direction and does not disclose the data or any "individually identifiable information" derived from it to anyone other than Google and does not use it for any purpose or (3) entity that uses covered information "only as reasonably necessary" to comply with law or enforce Google's terms of use or detect/prevent/mitigate fraud or security problems. *Id.* at "Definitions," #6.

who the third party is, and the purpose for the sharing.[44] It will also obtain "express affirmative consent" from the user for the sharing. [45]

Part III – Google Must Implement a Comprehensive Privacy Program

Under the proposed Consent Order, Google must create a "Comprehensive Privacy Program." The program must be designed to "address privacy risks" regarding "new and existing products and services" and to "protect the privacy and confidentiality of covered information." The Program must be documented in writing and be appropriate to the size, complexity, nature and scope of activities, and the sensitivity of the information.[46]

Google must designate employee(s) to be responsible for the program. Google must prepare a "privacy risk assessment." Privacy controls and procedures must be implemented to address risks identified in the risk assessment, and there must be regular testing and monitoring of effectiveness of those procedures. The program must be modified based on evolving risks, and Google is subject to a negligence standard. This Program applies to Google and other companies that provide services to Google.

Part IV – Google is Subject to Independent Assessments

Biennial assessments from a "qualified, objective, independent third-party professional" will be conducted. The person conducting the Assessment must be approved by the FTC. The first report is due in 180 days; subsequent reports are

[44] Other than sharing done for normal privacy policy purposes or terms of use.
[45] "Clearly and prominently" is defined as text that must be of a character that an ordinary consumer will see and understand, and that contrasts with background; oral communications that are done in a volume that an "ordinary consumer" can hear/understand; through video must also be written, be on screen for long enough, in predominant language. Must all be in understandable language and not be in contrary to or inconsistent with other statements.
[46] *Id.* at Section III.

due every two years for the next 20 years. The Assessment must explain the privacy controls implemented and how they are appropriate and meet Part III of the Agreement. [47]

Parts V – IX: Other requirements for Google

Google must make copies available to the FTC of: (1) all "widely disseminated statements" about Google's privacy protections (for 3 years); (2) all consumer complaints (for 6 months); (3) any documents that call compliance into question (for 5 years); and (4) materials relied upon to prepare assessments (for 3 years). [48]

Google must deliver the Agreement to all officers and directors who have supervisory responsibilities related to the Agreement. [49]

Google must notify the FTC thirty days before any major change in corporate structure or status that might affect compliance. If Google finds out less than 30 days before the action, it must tell the FTC as soon as is practicable. [50]

Google must file a report with the FTC in 90 days about how Google is complying with the Agreement.[51]

The Agreement will end in 20 years from issuance or from the most recent date a complaint is upheld due to a violation of the order. But filing a complaint will not affect any part of the Order that ends in less than 20 years, or the Order if the complaint is filed after the Order has ended. [52]

---

[47] *Id.* at Section IV.
[48] *Id.* at Section V.
[49] *Id.* at Section VI.
[50] *Id.* at Section VII.
[51] *Id.* at Section VIII.
[52] *Id.* at Section IX.

Commissioner Rosch's Concurrence

Commissioner J. Thomas Rosch accepted the Agreement, subject to final approval. But he expressed reservations about Part II of the Agreement and whether it is truly in the public's interest.[53] Commissioner Rosch argued in his concurrence that Google never represented that it would seek opt-in consent, so the opt-in requirement in Part II is entirely new and does not stem from any violation on Google's part. He expressed concern about the opt-in requirement being used as leverage in consent negotiations with other competitors.[54]

The provision in the Agreement regarding third-party sharing does not specify "material" sharing – just any new or additional sharing. Internet business models change fast and Part II is certain to apply to many companies and services. Also, Part II applies to all of Google's services and products, not just social networking. In Commissioner Rosch's opinion, Part II seems contrary to Google's self-interest and he is not comforted by the "fencing in" rationale.[55]

---

[53] Concurring Statement of Commissioner J. Thomas Rosch, In re Google Buzz, File No. 1023136, March 30, 2011, *available at* www.ftc.gov/os/caselist/1023136/110330googlebuzzstatement.pdf.
[54] *Id.*
[55] "Fencing in" order may cover legal conduct as long as it is "reasonably related" to the violation. *Jacob Siegel Co. v. FTC,* 327 U.S. 608 (1946).

V. EPIC's COMMENTS AND RECOMMENDATIONS

Under the Agreement with the FTC, Google agreed to adopt a "Comprehensive Privacy Program that "is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers and (2) protect the privacy and confidentiality of covered information." Consistent with those objectives, EPIC makes the following recommendations:

1) Require Fair Information Practices for all of Google's Products and Services

As a starting point for the requirements of a Comprehensive Privacy Program, EPIC recommends that the FTC require Google to adopt and implement the complete set of "Fair Information Practices." These would build on the principles of "transparency, user control, and security" previously endorsed by Google.[56] The Fair Information Practices that form the basis of such a Comprehensive Privacy Program should be modeled on the Privacy Act of 1974 and on the Organization for Economic Cooperation and Development ("OECD") Privacy Guidelines. The guidelines set out by the OECD include: data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. [57] The principles outlined in the Privacy Act are very similar.[58]

---

[56] *See, e.g.,* Testimony of Dr. Alma Whitten, Privacy Engineering Lead, Google Inc. Senate Committee on Commerce, Science, and Transportation Hearing on Consumer Online Privacy July 27, 2010, available at http://www.scribd.com/doc/34951271/Google-Testimony-Alma-Whitten.
[57] 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.
[58] Privacy Act of 1974, 5 USC § 552a.

2) Build a Do Not Track mechanism into the Chrome web browser

Google recently adopted an extension for its Chrome browser that would allow only for "opt-out of cookies" as opposed to more effective consent-based advertising. And Google has opposed the adoption of a formal Do Not Track mechanism in the browser itself.[59] Other companies, such as Microsoft, Apple, and Mozilla have added a Do Not Track mechanism to their browsers.[60] FTC Chairman Jon Leibowitz noted recently that Google is the lone holdout. "Apple just announced they're going to put it in their Safari browser. So that gives you Apple, Microsoft and Mozilla. Really the only holdout – the only company that hasn't evolved as much as we would like on this – is Google."[61]

Recommendation: The FTC should require Google, as part of its Comprehensive Privacy Program, to build a Do Not Track mechanism into its Chrome browser.

3) Encrypt all of its Cloud Computing Services

In March 2009, EPIC filed a complaint with the FTC regarding Google's cloud computing services.[62] 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

---

[59] "Keep Your Opt-Outs," Google Public Policy Blog, January 24, 2011, *available at* http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html.
[60] Gregg Keizer, "FTC Calls Out Google's Chrome Over Do Not Track," Computer World, April 20, 2011, *available at* http://www.computerworld.com/s/article/9215979/FTC_calls_out_Google_s_Chrome_over_Do_Not_Track?taxonomyId=70.
[61] *Id.*
[62] EPIC FTC Complaint, In re Google and Cloud Computing Services, Mar. 17, 2009, *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.

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 enjoining Google from offering such services until safeguards were verifiably established.[63] EPIC stated that such action by the Commission was necessary to ensure the safety and security of information submitted to Google by consumers, businesses, and federal agencies.[64]

The public has expressed similar concerns about the privacy implications of cloud computing. According to a Pew Internet & American Life Project report, 69% of Americans are making use of cloud computing.[65] 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.[66]

In February 2009, the World Privacy Forum (WPF) published a report on the risks to privacy and confidentiality from cloud computing which found that "a user's privacy and confidentiality risks vary significantly with the terms of service and

---

[63] *Id.*
[64] *Id.*
[65] 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.
[66] Penn, Schoen & Berland Associates, *Online Exposure, Offline Uncertainty: Privacy and Security in a Virtual World* (October 2009).

privacy policy established by the cloud provider."[67] 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."[68]

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.[69] Three other similar breaches involving Google cloud computing services all caused harm to consumers.[70] EPIC alleged that 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.[71] A letter from thirty-eight computer researchers and academicians to Google then-CEO Eric Schmidt raised similar concerns.[72]

Since then, consumers have become increasingly dependent on cloud computing services. According to a recent Pew Internet & American Life Project and Elon University study, most technology experts believe that the next decade will bring increased reliance on Internet-based applications and cloud computing.[73] The

---

[67] *Id.* at 6.
[68] *Id.*
[69] EPIC, "In the Matter of Google Inc, and Cloud Computing Services, Complaint and Request for Injunction, Request for Investigation and for Other Relief," before the Federal Trade Commission (Mar. 17, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.
[70] *Id.*
[71] *Id.*
[72] 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.
[73] Elon University and Pew Internet and American Life Project Survey, "The Future of the Internet, June 11, 2010, *available at*

survey found that the cloud computing brings considerable privacy and security risks.[74] 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 surprisingly, public officials with expertise in privacy matters are examining these services more closely to assess their impact on privacy and security.[75]

Recommendation: The FTC should examine closely Google's cloud computing practices, and should require Google as part of its Comprehensive Privacy Program to encrypt all of its cloud-based computing services.

4) Protect the Privacy and Anonymity of Google Book Search readers

The Google Book Search service collects an unprecedented amount of personal information that implicates reader privacy and intellectual freedom. EPIC, library organizations, and individuals specifically objected to the proposed Google Book Search settlement because it failed to adequately safeguard personal privacy.[76]

The court's opinion in the Google Book Search settlement opens the door to substantive privacy protections.[77] The Court acknowledged that parties expressed concern that the "digitization of books would enable Google to amass a huge collection of information, including private information about identifiable users,

---

http://www.elon.edu/docs/eweb/predictions/expertsurveys/2010survey/PIP_Future_of_internet_2010_cloud.pdf.

[74] *Id.*

[75] *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.

[76] *See, e.g.,* EPIC's Objection to the Proposed Settlement, (Sept. 8, 2009), *available at* http://epic.org/privacy/googlebooks/epic_objections_signed.pdf; EPIC: Google Books Settlement and Privacy, available at http://epic.org/privacy/googlebooks/.

[77] *See* The Authors Guild v. Google, Inc., 05 Civ. 8136-DC (SDNY 2011), *available at* http://www.nysd.uscourts.gov/cases/show.php?db=special&id=115.

without providing adequate protections regarding the use of such information."[78] The Court concluded that "The privacy concerns are real" and suggested that "certain additional privacy protections could be incorporated" in a revised settlement agreement.[79]

The Commission should fill this gap. It should require Google to institute practices in its Comprehensive Privacy Program that would assure reader confidentiality and anonymity when using the Google Book Search service. One of these practices should be to forbid Google from requiring users to register for and use a Google Account to access the wealth of information in the Google Book Search database.

Recommendation: The Commission should require that Google, as part of its Comprehensive Privacy Program, protect the privacy and anonymity of users of the Google Book Search service. In particular, the Commission should forbid Google from requiring Google Book Search users to have and use a Google Account.

5) Cease Tracking Mobile Phone Users' Locations or Web-Browsing Habits Without Explicit Opt-In Permission

Individuals are using location-based services that provide incentives for sharing where a person is at any given point in time. These location-based services are generally run on software applications found on GPS-enabled devices such as smart phones. The application requests the latitude and longitude of the user's phone or other GPS enabled device or from cell tower and Wi-Fi information.

[78] *Id.* at 13.
[79] *Id*. at 39-40.

The Pew Internet & American Life Project found that 35% of U.S. adults use phones able to run apps.[80] Location-based apps are focused on social-networking, consumer, and gaming activities. The Pew project also estimates that at least 1% of Internet users and 6% of all male Internet users are regularly taking advantage of location-based apps.[81]

Researchers recently discovered that Android phones collect location data every few seconds and send it to Google several times per hour.[82] The only way to opt out of this location tracking is to uncheck a box that is checked by default on Android phones.[83] Google has admitted to tracking users' location on its Android phones, but claims that the data is anonymous when the company receives it.[84] However, the data is tied to a phone's unique ID, and for phones that Google sells directly to users, such as the Nexus, Google will be able to associate personal information with that ID. The only way to change one's phone ID number is by performing a "factory reset" of the mobile device.[85]

Recommendation: The Commission should require Google, as part of its Comprehensive Privacy Program, to cease tracking mobile phone users' locations or web-browsing habits without explicit opt-in permission.

---

[80] Kristen Purcell et al., "The Rise of Apps Culture," Pew Internet, September 14, 2010, *available at* http://www.pewinternet.org/Reports/2010/The-Rise-of-Apps-Culture.aspx%5D.
[81] Kathryn Zickuhr and Aaron Smith, "4% of Online Americans use Location Based Services," Pew Internet, November 4, 2010, *available at* http://www.pewinternet.org/Reports/2010/Location-based-services.aspx
[82] Jennifer Valentino-Devries, "Google Defends Way it Gets Phone Data," The Wall Street Journal, April 23, 2011, *available at* http://online.wsj.com/article/SB10001424052748703387904576279451001593760.html.
[83] *Id.*
[84] *Id.*
[85] *Id.*

6) Require Search Warrants Before Sharing Data With Law Enforcement

Google and other Internet companies often receive subpoenas and National Security Letters from U.S. federal and state agencies that ask for the disclosure of customers' personal information that is in Google's possession. The release of personal information in these circumstances is inconsistent with the Fourth Amendment, the clear purpose of various federal privacy laws, and the legal protections afforded by other governments.[86]

Recommendation: As part of its Comprehensive Privacy Program, the FTC should require Google to limit the disclosure of user information to only those circumstances where a judge has determined (1) that there is clear and convincing evidence that the user is reasonably suspected of engaging in criminal activity; (2) that the information sought would be material evidence in the case; and (3) the user is afforded the opportunity to appear and contest such entity's claim.

7) Fully Delete User Search History and Other Information Collected After Six Months

Google products and services routinely retain extensive personal information for a much greater period of time than is needed to provide the service offered. For example,

Recommendation: The FTC should require that Google, as part of its Comprehensive Privacy Program, fully delete search history information linked to an identified or identifiable user after the search session is completed. Similar

[86] *See, e.g.,* Edmonton Public Schools, "Questions about the U.S. Patriot Act, privacy and access to personal information," *available at* https://sites.google.com/a/share.epsb.ca/shareepsbca-help/Home/privacy-matters/FAQ-privacy-and-US

limitations on data collection and retention should be established for other Google services.

8) Keep Non-Gmail Users' Emails Fully Private

Gmail subscribers consent to "content extraction" and analysis of their e-mail ("We serve highly relevant ads and other information as part of the service using our unique content-targeting technology," according to Gmail's privacy policy).[87] But non-subscribers who are emailing a Gmail user have not consented, and indeed may not even be aware that their communications are being analyzed or that a profile may be compiled on her. A lawsuit was filed in November 2010 over this issue arguing that by scanning non-Gmail users' email, Google is violating the Electronic Communications Privacy Act (ECPA).[88]

Recommendation: The FTC should require Google, as part of its Comprehensive Privacy Program, to keep non-Gmail users' emails fully private, and not scan them to provide targeted content to Gmail recipients.

9) End the Collection of Data Transmitted by Residential Wireless Routers

When Google began its Street View project in 2007, many privacy concerns were raised, but the debates focused almost exclusively on the collection and display of images obtained by the Google Street View digital cameras. It turns out that Google was also obtaining a vast amount of Wi-Fi data from Wi-Fi receivers that were concealed in the Street View vehicles. Following independent investigations,

[87] Google Privacy Policy, October 2010, *available at* http://www.google.com/intl/en/privacy/privacy-policy.html.
[88] Dan Goodin, "Google Sued for Scanning Emails of non-Gmail Users," The Register, November 23, 2010, *available at* http://www.theregister.co.uk/2010/11/23/gmail_privacy_lawsuit/.

Google now concedes that it gathered MAC addresses (the unique device ID for Wi-Fi hotspots) and network SSIDs (the user-assigned network ID name) tied to location information for private wireless networks. Google also admits that it has intercepted and stored Wi-Fi transmission data, which includes email passwords and email content.[89]

Although the FTC ended its investigation of Street View in October 2010, a more thorough review of the matter suggests that there were substantial privacy violations to be addressed.[90]

Recommendation: The FTC should require Google, as part of its Comprehensive Privacy Program, to suspend all Street View Wi-Fi data collection.

10) Make Results of Google's Privacy Assessments Available to the Public

Currently the Agreement does not require the results of Google's initial or biennial assessments to be public. It is important that the public knows what is in these assessments both as an added incentive for Google to comply and to further the goals of transparency and open government.

Recommendation: The FTC should make the results of Google's privacy program Assessments results public.

---

[89] *See generally*, EPIC, "Investigations of Google Street View,"" available at http://epic.org/privacy/streetview/

[90] CNN, "FTC ends Google 'Street View' investigation without fines," Oct. 27, 2010, *available at* http://articles.cnn.com/2010-10-27/tech/ftc.google.investigation_1_wi-fi-data-alan-eustace-google-maps?_s=PM:TECH, *but see* Joel Gurin, FCC Chief of the Consumer and Governmental Affairs Bureau ,"Consumer View: Staying Safe from Cyber Snoops," (June 11, 2010) ("Google's behavior also raises important concerns. Whether intentional or not, collecting information sent over WiFi networks clearly infringes on consumer privacy."), Amy Schatz and Amir Efrati, "FCC Investigating Google Data Collection," Wall Street Journal, Nov. 11, 2010; *See also,* EPIC Complaint to FCC Regarding Google Street View Data Collection (May 18, 2010), *available at* http://epic.org/privacy/cloudcomputing/google/EPIC_StreetView_FCC_Letter_05_21_10.pdf.

11) Apply the Provisions of its Agreement with Google to All Other Internet Companies

The Comprehensive Privacy Program set out in the Consent Order should apply to other Internet companies as well. This will raise the standards of consumer privacy for Internet users. This will also address the anti-trust concern that Commissioner Rosch identifies in his concurrence. [91]

Recommendation: The FTC should apply the provisions of its Agreement with Google to all Internet companies. If this cannot be done directly by means of the Consent Order, then it should be put forward by the FTC as a recommendation to Congress.

VI. CONCLUSION

EPIC supports the Consent Order set out by the FTC regarding the investigation In the Matter of Google, Inc., FTC File No. 102 3136.. These comments provide further detail for how best the Commission can require Google to discharge its obligation to create the "Comprehensive Privacy Program" set out in Part III of the Order.

Marc Rotenberg
EPIC President

Sharon Goott Nissim
EPIC Consumer Privacy Counsel

[91] Concurring Statement of Commissioner J. Thomas Rosch, In re Google Buzz, File No. 1023136, March 30, 2011, *available at* www.ftc.gov/os/caselist/1023136/110330googlebuzzstatement.pdf.Commissioner Rosch, Concurrence *In the Matter of* Google, *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzstatement.pdf.

Thomas H. Moore
EPIC Of Counsel

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave., NW
Suite 200
Washington, DC 20009
+1 202 483 1140 (tel)
+1 202 483 1248 (fax)