Appendix 11 – EPIC's FTC Feb. 16, 2010 Complaint in re: Google Buzz

Before the
Federal Trade Commission
Washington, DC

In the Matter of	)
	)
Google, Inc.	)
	)
	)

Complaint, Request for Investigation, Injunction, and Other Relief

I. Introduction

1. This complaint concerns an attempt by Google, Inc., the provider of a widely used email service to convert the private, personal information of Gmail subscribers into public information for the company's social network service Google Buzz. This change in business practices and service terms violated user privacy expectations, diminished user privacy, contradicted Google's own privacy policy, and may have also violated federal wiretap laws. In some instances, there were clear harms to service subscribers. These business practices are Unfair and Deceptive Trade Practices, subject to review by the Federal Trade Commission (the "Commission") under section 5 of the Federal Trade Commission Act.

2. These business practices impact more than 37 million users of Gmail who fall within the jurisdiction of the United States Federal Trade Commission.[1]

3. EPIC urges the Commission to investigate Google, determine the extent of the harm to consumer privacy and safety, require Google to provide Gmail users with opt-in consent to the Google Buzz service, require Google to give Gmail users meaningful control over personal information, require Google to provide notice to and request consent from Gmail users before making material changes to their privacy policy in the future, and seek appropriate injunctive and compensatory relief.

[1] Erick Schonfeld, *Gmail Nudges Past AOL Email in the U.S. to Take No. 3 Spot*, TechCrunch (Aug. 14, 2009), http://techcrunch.com/2009/08/14/gmail-nudges-past-aol-email-in-the-us-to-take-no-3-spot/.

II. Parties

4. The Electronic Privacy Information Center ("EPIC") is a not-for-profit research center based in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the Federal Trade Commission. Among its other activities, EPIC first brought the Commission's attention to the privacy risks of online advertising.[2] In 2004, EPIC filed a complaint with the FTC regarding the deceptive practices of data broker firm Choicepoint, calling the Commission's attention to "data products circumvent[ing] the FCRA, giving businesses, private investigators, and law enforcement access to data that previously had been subjected to Fair Information Practices."[3] As a result of the EPIC complaint, the FTC fined Choicepoint $15 million.[4] EPIC initiated the complaint to the FTC regarding Microsoft Passport.[5] The Commission subsequently required Microsoft to implement a comprehensive information security program for Passport and similar services.[6] EPIC also filed a complaint with the FTC regarding the marketing of amateur spyware,[7] which resulted in the issuance of a permanent injunction barring sales of CyberSpy's "stalker spyware," over-the-counter surveillance technology sold for individuals to spy on other individuals.[8]

---

[2] *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.

[3] *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.

[4] Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties*, $5 Million for Consumer Redress, http://www.ftc.gov/opa/2006/01/choicepoint.shtm (last visited Dec. 13, 2009).

[5] *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.

[6] *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 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.

[7] *In the Matter of Awarenesstech.com, et al.*, Complaint and Request for Injunction, Request for Investigation and for Other relief, before the Federal Trade Commission, *available at* http://epic.org/privacy/dv/spy_software.pdf.

[8] FTC v. Cyberspy Software, No. 6:08-cv-1872 (D. Fla. Nov. 6, 2008) (unpublished order), *available at* http://ftc.gov/os/caselist/0823160/081106cyberspytro.pdf.

5. In March 2009, EPIC urged the FTC to undertake an investigation of Google and cloud computing.[9] In that complaint, EPIC specifically warned the FTC that Google had failed to take appropriate steps to safeguard the privacy and security of users. The FTC agreed to review the complaint, stating that it "raises a number of concerns about the privacy and security of information collected from consumers online."[10] However, to date, the FTC has announced no formal action in the Google cloud computing matter.

6. Google, Inc. was founded in 1998 and is based in Mountain View, California. Google's headquarters are located at 1600 Amphitheatre Parkway, Mountain View, CA 94043. At all times material to this complaint, Google's course of business, including the acts and practices alleged herein, has been and is in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 45.

The Importance of Email Privacy

7. Law, technology, business practice, and custom treat emails and associated information as fundamentally private.

8. While email senders and recipients always have an opportunity to disclose email-related information to third parties, email service providers have a particular responsibility to safeguard the personal information that subscribers provide.

9. Improper disclosure of even a limited amount of subscriber information by an email service provider can be a violation of both state and federal law.

10. An attempt by an email service provider to attempt to convert the personal information of all of its customers into a separate service raises far-reaching concerns for subscribers and implicates both consumer and personal privacy interests.

The Release of Google Buzz

11. Google launched Google Buzz on Tuesday, February 9, 2010. Google Buzz is a social networking tool linked to a user's Gmail email account, where users "start conversations about the things you find interesting."[11]

---

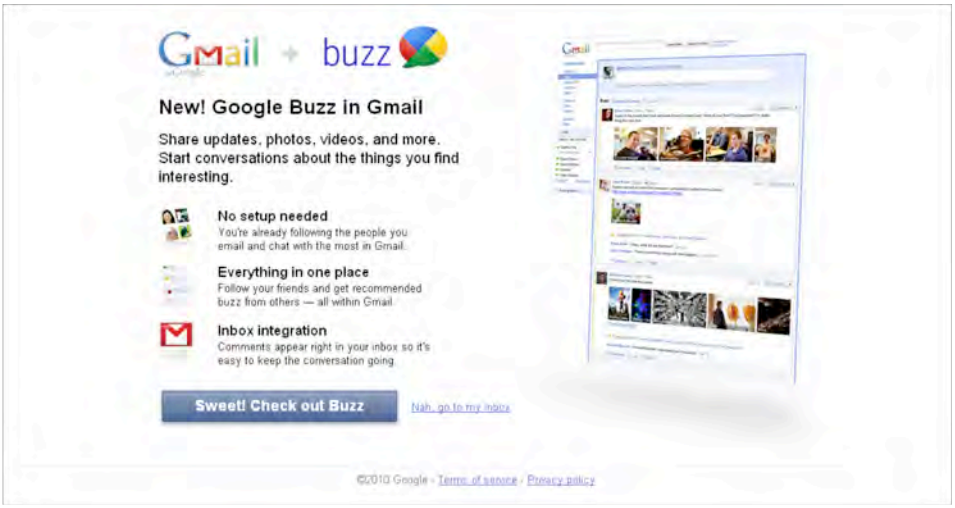
[9] *In the Matter of Google, Inc., and Cloud Computing Services*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Mar. 17, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.

[10] Letter from Eileen Harrington, Acting Director of the FTC Bureau of Consumer Protection, to EPIC (Mar. 18, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/031809_ftc_ltr.pdf.

[11] Todd Jackson, Google Blog post: *Introducing Google Buzz* (Feb. 9, 2010), http://googleblog.blogspot.com/2010/02/introducing-google-buzz.html.

12. When Google Buzz was introduced, users could not choose whether to sign up for the tool. According to Google, "No setup needed. Automatically follow the people you email and chat with most in Gmail."[12]

13. After the launch of Google Buzz, Gmail users who signed into Gmail were confronted with the following screen:



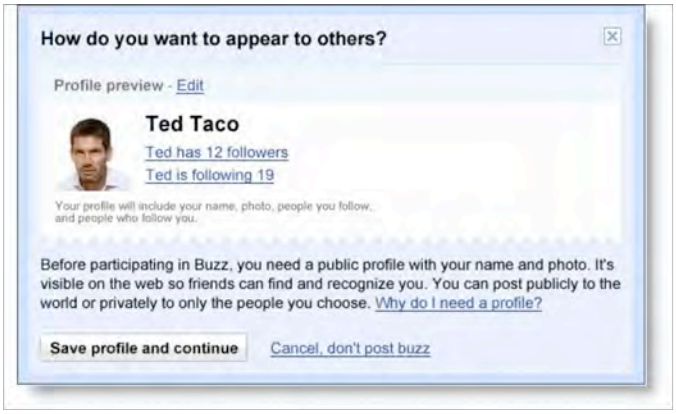
14. Regardless of whether a user clicked the button labeled "Sweet! Check out Buzz" or "Nah, go to my inbox," Google Buzz was activated.

15. Once Google Buzz was activated, the tool automatically populated a user's "following" lists using that user's most frequent email contacts.

16. Google Buzz did not warn users that their email contacts would be used to populate their "following" lists.

17. Once users clicked on the "Buzz" tab in Gmail, and then on the text box to share a new post, users were met with the following screen:

[12] Google Buzz Page, http://www.google.com/buzz (last visited Feb. 12, 2010).



18. Once users created public profiles, their "following" and "followed by" lists were also automatically visible to the public.

19. Users were not explicitly warned that their lists would be automatically visible to the public. Instead, each user was told only that "Your profile will include your name, photo, people you follow, and people who follow you." A separate section of the notice stated that the profile was "visible on the web so friends can find and recognize you."

20. Users could hide their "following" and "followed by" lists only by clicking through several links to edit their public profile and then unchecking the box labeled "Display the list of people I'm following and people following me."

Google's Disclosure of Users' Email Contacts

21. Gmail contact lists routinely include deeply personal information, including the names and email addresses of estranged spouses, current lovers, attorneys and doctors.

22. The frequency with which a user communicates with a given contact is also deeply personal and demonstrates the closeness of the user's relationship with that contact.

23. The activation of Buzz disclosed not only portions of users' contact lists, but more specifically disclosed the contacts with whom users communicate most often.

24. The fact that the auto-following lists were composed of users' most common Gmail contacts was widely known and publicized, as well as easily deduced by individual

users.[13] As such, anyone looking at a newly-activated Buzz user's "following" list would know that the list indicated which people that user communicated with most often.

User Opposition to Google Buzz

25. Since the introduction of Google Buzz, Google has been met with widespread criticism and user opposition to the service. Nicholas Carlson, senior editor of the Silicon Alley Insider, wrote an article discussing Google Buzz's "huge privacy flaw."[14] Carlson wrote,

> The problem is that—by default—the people you follow and the people that follow you are made public to anyone who looks at your profile. In other words, before you change any settings in Google Buzz, someone could go into your profile and see the people you email and chat with the most.[15]

Carlson's article was viewed over 400,000 times, drew in over 250 comments from readers, and was tweeted nearly 6,000 times.

26. CNET writer Molly Wood also wrote against Google Buzz's default settings:

> First, you automatically follow everyone in your Gmail contact list, and that information is publicly available in your profile, by default, to everyone who visits your profile. It's available with helpful "follow" links too—wow, you can expand your Buzz network *so fast* by harvesting the personal contact lists of other people!

Wood continued, speaking of the privacy invasion associated with Google Buzz's attempt to publicize private information in which users have an expectation of privacy:

> But I *do* have an expectation of privacy when it comes to my e-mail, and I think that even in this age of social-networking TMI, most people still think of e-mail as a safe place for speaking privately with friends and family. And for Google to come along and broadcast that network to the world without asking first—and force you to turn it off after the fact—is, I think, both shocking and unacceptable.

---

[13] *See* User Opposition to Google Buzz, *infra* ¶¶ 25–30.
[14] Nicholas Carlson, *WARNING: Google Buzz Has a Huge Privacy Flaw*, Silicon Alley Insider (Feb. 10, 2010), http://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2.
[15] *Id.*

27. One Yahoo! Fellow at the Institute for the Study of Diplomacy at Georgetown University foresaw that Google Buzz could be a "tragic privacy disaster for Google, potentially of the same magnitude that Beacon was to Facebook."[16] He described the serious threats that could occur from publicly sharing a user's Gmail contacts:

> I am extremely concerned about hundreds of activists in authoritarian countries who would never want to reveal a list of their interlocutors to the outside world. Why so much secrecy? Simply because many of their contacts are other activists and often even various "democracy promoters" from Western governments and foundations. Many of those contacts would now inadvertently be made public.
>
> . . . .
>
> But potential risk from disclosing such data extends far beyond just supplying authoritarian governments with better and more actionable intelligence. For example, most governments probably already suspect that some of their ardent opponents are connected to Western organizations but may lack the evidence to act on those suspicions. Now, thanks to Google's desire to make an extra buck off our data, they would finally have the ultimate proof they needed (if you think that this is unrealistic, consider this: the Iranian authorities have once used membership in an academic mailing list run out of Columbia as evidence of spying for the West).[17]

28. Anonymous blogger "Harriet Jacobs" described another type of threat resulting from creating automated lists from email contacts:

> I use my private Gmail account to email my boyfriend and my mother.
>
> There's a BIG drop-off between them and my other "most frequent" contacts.
>
> You know who my third most frequent contact is?
>
> My abusive ex-husband.
>
> Which is why it's SO EXCITING, Google, that you AUTOMATICALLY allowed all my most frequent contacts access to my Reader, including all the comments I've made on Reader items, usually shared with my boyfriend, who

---

[16] Evgeny Morozov, Foreign Policy Net.Effect Blog Post: *Wrong Kind of Buzz around Google Buzz* (Feb. 11, 2010), http://neteffect.foreignpolicy.com/posts/2010/02/11/wrong_kind_of_buzz_around_google_buzz.
[17] *Id.*

> I had NO REASON to hide my current location or workplace from, and never did.[18]

Jacobs' story received international attention and was cited in numerous articles and blog posts that discussed the privacy concerns associated with Google Buzz, including the New York Times,[19] CNET,[20] The Telegraph,[21] and The Guardian.[22]

29. Texas lawyer Don Cruise also took issue with creating automated social networking lists from email contacts, describing Google's actions as "[r]epurposing old data in a way that flouts our expectations of privacy."[23] Cruise describes the problem this poses for professional confidentiality obligations:

> There was a pretty massive shift in your privacy a couple of days ago. You might not have noticed it. But unless you take a few steps to protect yourself, Google may be sharing some of your confidences with the world.
>
> . . . .
>
> Assume for just a moment that this concerns you. Assume, perhaps, that some other people might expect to be able to contact you in confidence—as a lawyer, a blogger, a journalist, or even (gasp) a friend. Assume that part of your professional responsibility is keeping the confidences of others.

Cruise offers four tips to protecting confidentiality in relationships, including the fact that "when you "turn off" Google Buzz, that doesn't actually remove your information from search results."[24] Rather, updates are hidden, although all other information is still shared.[25]

---

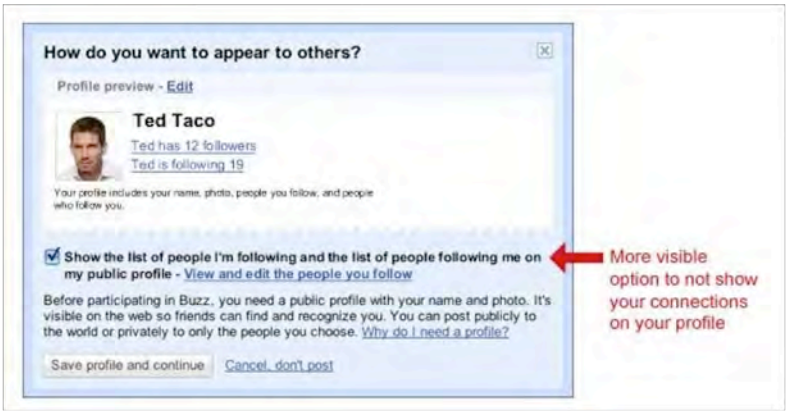
[18] Harriet Jacobs, Fugitivus Blog Post: *Fuck You Google* (Feb. 11, 2010), http://gizmodo.com/5470696/fck-you-google.
[19] Miguel Helft, *Critics Say Google Invades Privacy with New Service*, N.Y. Times (Feb. 12, 2010), *available at* http://www.nytimes.com/2010/02/13/technology/internet/13google.html.
[20] Tom Krazit, *More Google Buzz Tweaks, Separate Version Coming?*, CNET News (Feb. 12, 2010), http://news.cnet.com/8301-30684_3-10453027-265.html.
[21] Shane Richmond, *Google Buzz Tweaked after User Concerns,* Telegraph (Feb. 12, 2010), http://blogs.telegraph.co.uk/technology/shanerichmond/100004650/google-buzz-tweaked-after-user-concerns/.
[22] Charles Arthur, Guardian Technology Blog Post: *Google Buzz's Open Approach Leads to Stalking Threat* (Feb. 12, 2010), http://www.guardian.co.uk/technology/blog/2010/feb/12/google-buzz-stalker-privacy-problems.
[23] Don Cruise, The Supreme Court of Texas Blog Post: *Lawyers (or Journalists) with Gmail Accounts: Careful with the Google Buzz* (Feb. 11, 2010), http://www.scotxblog.com/legal-tech/lawyer-privacy-on-google-buzz/.
[24] *Id.*
[25] *Id.*

30. Several articles have surfaced containing information listing Buzz's privacy concerns. One such article described these three main concerns: 1) Google Buzz automatically imports contacts and shows them as friends, 2) Google Buzz grabs photos without a user uploading them, and 3) Google Buzz can pinpoint and broadcast your exact location.[26]

First Round of Changes to Google Buzz

31. On the afternoon of February 11, 2010, in response to user criticism, Google made changes to the Google Buzz tool.[27]

32. Google still requires users to opt out of using the Google Buzz service. When a user first clicks on the text box to write a post, a pop-up screen appears. On this screen, there is a checked box next to the option: "Show the list of people I'm following and the list of people following me on my public profile." To prevent this from occurring, a user must uncheck the box, or in other words "opt out" of sharing. For a screenshot of this window, see below.

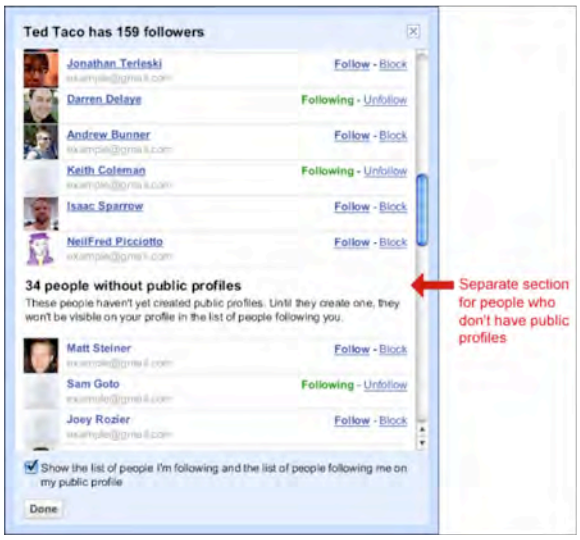


33. Google changed which of a user's connections appear on the user's public profile. Only contacts who have created a public profile will appear on a user's public follower list. Users who have not created a public profile will still be on a user's follower list, but such contacts will not be public, and cannot be seen by other contacts. For an example of this distinction, see the screenshot below:

---

[26] Andrew R. Hickey, *3 Google Buzz Privacy Concerns*, ChannelWeb (Feb. 11, 2010), http://www.crn.com/software/222900037.

[27] Todd Jackson, Gmail Blog Post: *Millions of Buzz Users, and Improvements Based on your Feedback* (Feb. 11, 2010), http://gmailblog.blogspot.com/2010/02/millions-of-buzz-users-and-improvements.html.



34. Google still compiled a user's "following lists" based on personal address contacts and chat list contacts.

35. Google still did not notify users from the outset that Google creates the list of "people you follow" and "people who follow you" according to the frequency of conversation between a user and contacts in the user's Gmail address book or chat list. Therefore, users remained unaware that showing this list amounts to publishing their address book and Gmail contacts list.

36. On the pop-up screen that appears before writing a post, Google still did not clearly state that showing the user's connection means showing connections publicly to everyone, and having them publicly indexed by search engines. The checked box only states, "Show the list of people I'm following and the list of people following me on my profile."

Continued User Opposition to Google Buzz

37. Nicholas Carlson, with Silicon Alley Insider, observed that even with the changes, Google failed to recognize the privacy risks to normal users:

> We have a message for the brilliant people behind Google Buzz (and the rest of Google's products): the rest of the world is NOT like you. These privacy

> concerns aren't for the incredibly computer savvy, the patient beta testers, or Twitter and Facebook power users.[28]

He urged Google to make the sharing of lists opt-in rather than opt-out, and to more clearly explain to users exactly what Google Buzz shares.

38. Similarly, Robin Wauters, with Tech Crunch, argued that the changes were insufficient:

> Even with the improvements that were made to the Buzz product, Google is confusing the hell out of people here—and make some lives hell for them to boot.[29]

39. CNET's Tom Krazit reported on the reaction to Google Buzz's privacy risks:

> The privacy backlash certainly hurt the perception of Google and Google Buzz during the first week of the service. Those already skeptical of Google's insatiable thirst for data and its attitudes toward privacy could not help but see Google's decisions on the controls for Buzz profiles as a way of tricking people into generating public content.[30]

He argued that Google could help address privacy concerns by adding Google Buzz to the Google Privacy Dashboard.

40. Finally, Kevin Purdy, with Lifehacker, argued that the changes fail to protect the users who had already activated Google Buzz:

> Google touts in the same post the "tens of millions of people" who have logged into Buzz in some way, creating 9 million posts and comments, and those folks have to discover the non-public option on their own.[31]

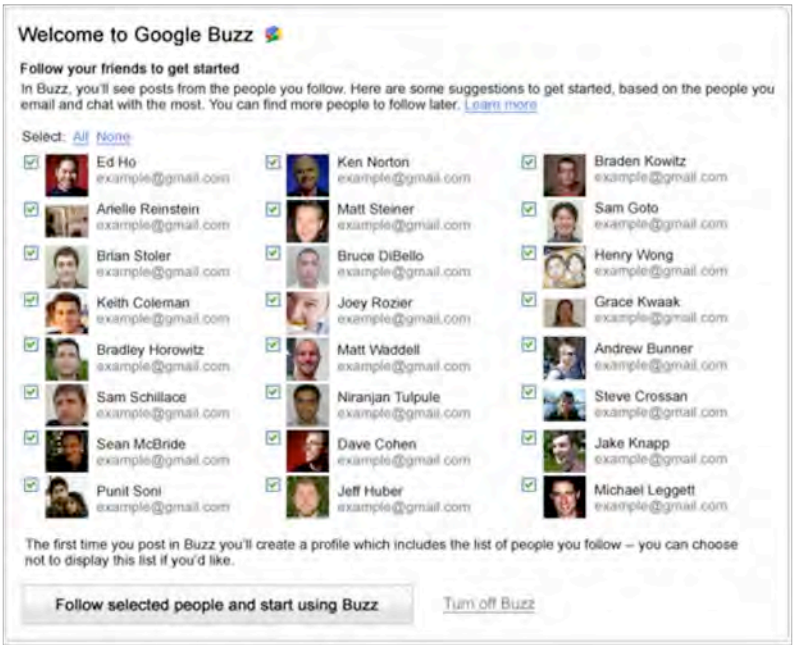
---

[28] Nicholas Carlson, *Google Buzz Still Has Major Privacy Flaw*, Silicon Alley Insider, Feb. 12, 2010, http://www.businessinsider.com/googles-nice-improvements-to-buzz-dont-correct-major-privacy-flaw-2010-2.
[29] Robin Wauters, *Google Buzz Privacy Issues Have Real Life Implications*, Tech Crunch, Feb. 12, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/12/AR2010021201490.html.
[30] Tom Krazit, *Google tweaks Buzz privacy settings*, CNET, Feb. 11, 2010, http://news.cnet.com/8301-30684_3-10452412-265.html.
[31] Kevin Purdy, *Google Updates, Explains Buzz Privacy Setup*, Lifehacker, Feb. 11, 2010, http://lifehacker.com/5470104/google-updates-explains-buzz-privacy-setup.

Google Buzz's Second Round of Changes

41. On February 13, 2010, in response to continued user criticism, Google made more changes to Google Buzz in an effort to address privacy concerns.[32]

42. Google is now using an auto-suggest model, rather than an auto-follow model. In other words, "You won't be set up to follow anyone until you have reviewed the suggestions and clicked 'Follow selected people and start using Buzz.'"[33] For a screenshot of the new welcome page for Google Buzz, see below.[34]



43. Google Buzz still populates the suggested social networking list of people a user follows based on frequent address book and chat contacts. Although the "welcome page" states that "[y]ou can find more people to follow later," the contacts from a user's address book and chat list make up a user's initial "follow" list.

---

[32] Todd Jackson, Google Blog Post: *A New Buzz Start-up Experience Based on your Feedback* (Feb. 13, 2010), http://gmailblog.blogspot.com/2010/02/new-buzz-start-up-experience-based-on.html.
[33] *Id.*
[34] *Id.*

44. Google Buzz still allows people to automatically follow a user. The burden remains on the user to block those unwanted followers. As a CNET article explained, "It will give those who acquiesced to Google's sleight of software another chance to review those automatically chosen to be followed, just to check whether there might some unwanted ex-husbands, ex-girlfriends, or slightly insane stalkers that slipped through the net."[35]

45. The "welcome screen" does not make clear that the user must create a profile that would be public and indexed by search engines. The screen only states, "The first time you post in Buzz you'll create a profile which includes the list of people you follow—you can choose not to display this list if you'd like."

46. Google has not announced any changes to the pop-up screen that appears when a user initially posts on Google Buzz. Users are still unaware that showing the user's connection means showing connections publicly to everyone, and having them publicly indexed by search engines.

III. Legal Analysis

The FTC's Section 5 Authority

47. Google is engaging in unfair and deceptive acts and practices.[36] Such practices are prohibited by the FTC Act, and the Commission is empowered to enforce the Act's prohibitions.[37] These powers are described in FTC Policy Statements on Deception[38] and Unfairness.[39]

48. A trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[40]

---

[35] Chris Matyszczyk, *Google Changes Buzz Privacy Settings – Again*, CNET News (Feb. 14, 2010), http://news.cnet.com/8301-17852_3-10453274-71.html.
[36] *See* 15 U.S.C. § 45.
[37] *Id.*
[38] Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), *available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm* [*hereinafter* FTC Deception Policy].
[39] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm [*hereinafter* FTC Unfairness Policy].
[40] 15 U.S.C. § 45(n); *see, e.g.*, *Fed. Trade Comm'n v. Seismic Entertainment Productions, Inc.*, Civ. No. 1:04-CV-00377 (Nov. 21, 2006) (finding that unauthorized changes to users' computers that affected the functionality of the computers as a result of Seismic's anti-spyware software constituted a "substantial injury without countervailing benefits.").

49. The injury must be "substantial."[41] Typically, this involves monetary harm, but may also include "unwarranted health and safety risks."[42] Emotional harm and other "more subjective types of harm" generally do not make a practice unfair.[43] Secondly, the injury "must not be outweighed by an offsetting consumer or competitive benefit that the sales practice also produces."[44] Thus the FTC will not find a practice unfair "unless it is injurious in its net effects."[45] Finally, "the injury must be one which consumers could not reasonably have avoided."[46] This factor is an effort to ensure that consumer decision making still governs the market by limiting the FTC to act in situations where seller behavior "unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."[47] Sellers may not withhold from consumers important price or performance information, engage in coercion, or unduly influence highly susceptible classes of consumers.[48]

50. The FTC will also look at "whether the conduct violates public policy as it has been established by statute, common law, industry practice, or otherwise."[49] Public policy is used to "test the validity and strength of the evidence of consumer injury, or, less often, it may be cited for a dispositive legislative or judicial determination that such injury is present."[50]

51. The FTC will make a finding of deception if there has been a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[51]

52. First, there must be a representation, omission, or practice that is likely to mislead the consumer.[52] The relevant inquiry for this factor is not whether the act or practice actually

---

[41] FTC Unfairness Policy, *supra* note 113.
[42] *Id.*; *see, e.g.*, *Fed. Trade Comm'n v. Information Search, Inc.*, Civ. No. 1:06-cv-01099 (Mar. 9, 2007) ("The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers' authorization causes substantial harm to consumers and the public, including, but not limited to, endangering the health and safety of consumers.").
[43] FTC Unfairness Policy, *supra* note 113.
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] FTC Deception Policy, *supra* note 112.
[52] FTC Deception Policy, *supra* note 112; *see, e.g.*, *Fed Trade Comm'n v. Pantron I Corp.*, 33 F.3d 1088 (9th Cir. 1994) (holding that Pantron's representation to consumers that a product was effective at reducing hair loss was materially misleading, because according to studies, the success of the product could only be attributed to a placebo effect, rather than on scientific grounds).

misled the consumer, but rather whether it is likely to mislead.[53] Second, the act or practice must be considered from the perspective of a reasonable consumer.[54] "The test is whether the consumer's interpretation or reaction is reasonable."[55] The FTC will look at the totality of the act or practice and ask questions such as "how clear is the representation? How conspicuous is any qualifying information? How important is the omitted information? Do other sources for the omitted information exist? How familiar is the public with the product or service?"[56]

53. Finally, the representation, omission, or practice must be material.[57] Essentially, the information must be important to consumers. The relevant question is whether consumers would have chosen another product if the deception had not occurred.[58] Express claims will be presumed material.[59] Materiality is presumed for claims and omissions involving "health, safety, or other areas with which the reasonable consumer would be concerned."[60] The harms of this social networking site's practices are within the scope of the FTC's authority to enforce Section 5 of the FTC Act and its purveyors should face FTC action for these violations.

IV. Prayer for Investigation and Relief

54. EPIC requests that the Commission investigate Google, enjoin its unfair and deceptive business practices, and require Google to protect the privacy of Gmail users. Specifically, EPIC requests the Commission to:

    Compel Google to make Google Buzz a fully opt-in service for Gmail users;

    Compel Google to cease using Gmail users' private address book contacts to compile social networking lists;

    Compel Google to give Google Buzz users more control over their information, by allowing users to accept or reject followers from the outset; and

    Provide such other relief as the Commission finds necessary and appropriate.

---

[53] FTC Deception Policy, *supra* note 112.
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.*

55. EPIC reserves the right to supplement this petition as other information relevant to this proceeding becomes available.

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director
Kimberly Nguyen, EPIC Consumer Privacy Counsel
Jared Kaprove, EPIC Domestic Surveillance Counsel

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