



them to make certain information about themselves public and to link to their content on Google product websites, such as the user's Google Reader shared items, public Picasa Web Albums, and Blogger blog. Information on a consumer's public Google profile, which may include the consumer's name, location, and photo, is available on the Internet and may be indexed by search engines.

### **RESPONDENT'S STATEMENTS**

6. Respondent has disseminated or caused to be disseminated statements to consumers on its website regarding its privacy practices, including but not limited to:
  - a. From approximately October 2004 until October 2010, the following statement in the Gmail Privacy Policy about Google's use of consumer information provided through Gmail:
  - b. From approximately October 2005 until October 2010, the following statement in Google's Privacy Policy regarding consumers' choices about the uses of their personal information in all of Google's products, including Gmail:

Gmail stores, processes and maintains your messages, contact lists and other data related to your account in order to provide the service to you.

When you sign up for a particular service that requires reg



- b. When first attempting to post in Buzz, users were directed to click through a profile creation screen, which explained that users needed to create a public Google profile before participating in Buzz. The profile creation screen contained the following header: “How do you want to appear to others?” The screen also included the following language in prominent, contrasting type: “Before participating in Buzz, you need a public profile with your name and photo. It’s visible on the web so friends can find and recognize you. You can post publicly to the world or privately to only the people you choose.” The profile creation screen also included the following language in small gray letters against a white background: “Your profile will include your name, photo, people you follow and people who follow you.” **Exhibit C** shows how the profile creation screen appeared to consumers.
  - c. In order to find controls that would allow the user to stop following certain individuals, a user had to take the additional step to click a link marked “edit,” which expanded the profile creation screen. Only after clicking “edit” could users choose not to have their lists of followers and people the user was following shown on the user’s public Google profile. They did so by unchecking a pre-checked box. Users who saw no reason to edit their profile – particularly those who already had created a Google profile and did not realize new information would be added and publicly available by default on that profile – would never have learned that these controls were available. **Exhibit D** shows how the expanded profile creation screen appeared to consumers.
  - d. The default setting for items posted in Google Buzz was “public” – shared with all of a user’s followers – though users had the ability to select “private” from a drop-down menu to post to a more limited group. Public buzzes were added to a user’s public Google profile, which was searchable on the Internet and could be indexed by search engines.
  - e. Google Buzz also automatically connected to other information users had made public through Google products such as Picasa and Reader. In many instances, this information was automatically compiled and broadcast in public buzzes that showed up on the user’s public Google profile.
10. Certain personal information of Gmail users was shared without consumers’ permission through the Google Buzz social network.
- a. In some cases, Gmail users had previously blocked certain email contacts from viewing other information about them, but those preferences were not carried over to Buzz. For example, even if a Gmail user blocked an individual in Google Chat or Google Reader, that person was not blocked in Buzz and could show up as a follower of that Gmail user.

- b. Users could not block followers who did not have a public Google profile. Moreover, an individual who had not provided a first or last name when setting up a Google account would appear as an “unknown” follower to a user. The user was not only unable to block such an individual from following them, but they had no way of knowing the individual’s identity.
  - c. If a Google Buzz user wanted to reply or direct a comment to an individual, the user placed the @ sign in front of the individual’s name, and Google suggested names from a user’s contact list. If the user selected a name or account from the suggest list that was not associated with a Google profile, Buzz filled in the field with that person’s private email address. Using an individual’s private email address in a public reply or comment thus exposed the address to all followers of the user and allowed that email address to be accessed by search engines.
11. In response to the launch of Google Buzz, many users complained about the automatic generation of lists of followers and people to follow from email contact lists that included in some cases: individuals against whom they had obtained restraining orders; abusive ex-husbands; clients of mental health professionals; clients of attorneys; children; and recruiters they had emailed regarding job leads. Further, because of the default settings and the complex and multi-step nature of respondent’s disclosures described in **paragraph 9**, consumers were confused about what information was made public through Buzz and complained about the potential disclosure of private email addresses.
12. Following widespread public criticism and thousands of consumer complaints, Google made certain changes to the Buzz service. Among other things, Google: (1) gave users the ability to effectively disable or turn off Buzz; (2) switched from setting up Gmail users with an automatic list of people to follow to suggesting a list of people to follow for users to approve; (3) made the process for editing lists of followers and people to follow clearer and more easily accessible; (4) made it possible for users to block any follower, regardless of whether that follower had a public profile; (5) made the option not to show lists of followers on a user’s public profile more prominent; (6) discontinued the feature that automatically connected to information from other websites, such as Picasa and Google Reader; and (7) ~~offered~~ ~~to~~ ~~provide~~ ~~users~~ ~~with~~ ~~an~~ ~~option~~ ~~to~~ ~~block~~ ~~any~~ ~~followers~~ ~~and~~ ~~people~~ ~~to~~ ~~follow~~ ~~from~~ ~~their~~ ~~email~~ ~~contact~~ ~~lists~~ ~~that~~ ~~included~~ ~~in~~ ~~some~~ ~~cases~~ ~~:~~ ~~individuals~~ ~~against~~ ~~whom~~ ~~they~~ ~~had~~ ~~obtained~~ ~~restraining~~ ~~orders~~ ~~;~~ ~~abusive~~ ~~ex-husbands~~ ~~;~~ ~~clients~~ ~~of~~ ~~mental~~ ~~health~~ ~~professionals~~ ~~;~~ ~~clients~~ ~~of~~ ~~attorneys~~ ~~;~~ ~~children~~ ~~;~~ ~~and~~ ~~recruiters~~ ~~they~~ ~~had~~ ~~emailed~~ ~~regarding~~ ~~job~~ ~~leads~~ ~~.~~ ~~Further~~ ~~,~~ ~~because~~ ~~of~~ ~~the~~ ~~default~~ ~~settings~~ ~~and~~ ~~the~~ ~~complex~~ ~~and~~ ~~multi-step~~ ~~nature~~ ~~of~~ ~~respondent’s~~ ~~disclosures~~ ~~described~~ ~~in~~ ~~paragraph~~ ~~9~~ ~~,~~ ~~consumers~~ ~~were~~ ~~confused~~ ~~about~~ ~~what~~ ~~information~~ ~~was~~ ~~made~~ ~~public~~ ~~through~~ ~~Buzz~~ ~~and~~ ~~complained~~ ~~about~~ ~~the~~ ~~potential~~ ~~disclosure~~ ~~of~~ ~~private~~ ~~email~~ ~~addresses~~ ~~.~~

networking service. Therefore, the representations set forth in **paragraph 13** were, and are, false or misleading and constitute a deceptive act or practice.

15. As set forth in **paragraph 6(b)**, respondent has represented, expressly or by implication, that it would seek consumers' consent to use information they provided for a purpose other than that for which it was collected.
16. In truth and in fact, as described in **paragraphs 7-11**, respondent did not seek consumers' consent before using the information they provided in connection with Gmail for the Google Buzz social networking product. Therefore, the representations set forth in **paragraph 15** were, and are, false or misleading and constitute a deceptive act or practice.
17. As set forth in **paragraph 8**, by offering the option "Nah, go to my inbox," as well as the option to "Turn off Buzz," respondent has represented, expressly or by implication, that consumers who clicked on these options would not be enrolled in Buzz.
18. In truth and in fact, as described in **paragraph 8**, consumers who clicked on these options were enrolled in certain features of Buzz. Therefore, the representations set forth in **paragraph 17** were, and are, false and misleading and constitute a deceptive act or practice.
19. As set forth in **paragraph 9**, respondent represented, expressly or by implication, through the Buzz enrollment screens and statements such as "How do you want to appear to others?" that consumers would be able to exercise control over what information would be made public through their Google public profile. Respondent failed to disclose, or failed to disclose adequately, that in most instances the contacts with whom users emailed and chatted the most would become public by default and that user information submitted through other Google products would be automatically broadcast through Buzz. These facts would be material to consumers in their enrollment in and use of the Google Buzz service. Therefore, respondent's failure to adequately disclose these facts, in light of the representations made, was, and is, a deceptive act or practice.

#### U.S.-EU SAFE HARBOR FRAMEWORK

tted

20. The U.S.-EU Safe Harbor Framework provides a method for U.S. companies to transfer personal data outside of the European Union ("EU") that is consistent with the requirements of the European Union Data Protection Directive ("Data Protection Directive").

21. To satisfy the EU's adequacy standard for certain commercial transfers, the U.S. Department of Commerce ("Commerce") and the EC negotiated the U.S.-EU Safe Harbor Framework, which went into effect in 2000. The Safe Harbor is a voluntary framework that allows U.S. companies to transfer personal data lawfully from the EU to the U.S. To join the Safe Harbor, a company must self-certify to Commerce that it complies with seven principles and related requirements that have been deemed to meet the EU's adequacy standard.

ki00 TD()Tj3.6000 0.00000 zf000

22. The Safe Harbor privacy principles, issued by Commerce on July 21, 2000, include the following:

**NOTICE:** An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

**CHOICE:** An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

23. From October 2005 until the present, Google has maintained a current self-certification to Commerce and has appeared on the list of Safe Harbor companies on the Commerce website. Prior to the launch of the Buzz social networking product, Google transferred data collected from Gmail users in Europe to the United States for processing.

24. From approximately October 2005 until the present, Google made the following statement in its Privacy Policy regarding its participation in the U.S.-EU Safe Harbor Framework:

Google adheres to the US Safe Harbor P00 TD(u TD(lem6400 0.0000 TD()Tj2.83.0000 TDfdww5e

