

Complaint

IN THE MATTER OF

GOOGLE, INC.CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECS. 5(A) OF THE FEDERAL TRADE COMMISSION ACT

Docket No. C-4336; File No. 102 3136
Filed, October 13, 2011 — Decision, October 13, 2011

This consent order addresses allegations that Google, Inc. provided inadequate privacy disclosures in violation of the FTC Act. In 2010, Google launched a social networking service called Google Buzz that allowed users to share updates, comments, photos, videos, and other information through posts or “buzzes.” The Google Buzz platform was available to consumers who signed up for Gmail, Google’s web-based email product. The complaint alleges that Google violated the FTC Act (1) by failing to advise Gmail users that its information would become public by default through Google Buzz; (2) by deceiving consumers about their ability to decline enrollment in certain features of Google Buzz; and (3) by misrepresenting its compliance with certain international data transfer laws. The order prohibits Google from misrepresenting the privacy and confidentiality of its users’ information. The order further requires Google to provide any user with clear and prominent notice and to obtain express affirmative consent prior to sharing the user’s information with any third party, under certain conditions. The order further requires Google to establish and maintain a comprehensive privacy program., and that Google obtain an independent, third-party assessment of its privacy practices every other year for the next 20 years.

Participants

For the *Commission*: *Katherine Race Brin and Kathryn D. Ratté.*

For the *Respondent*: *Al Gidari, Perkins Coie.*

COMPLAINT

The Federal Trade Commission, having reason to believe that Google Inc. (“Google” or “respondent”), a corporation, has violated the Federal Trade Commission Act (“FTC Act”), and it appearing to the Commission that this proceeding is in the public interest, alleges:

Complaint

1. Respondent Google is a Delaware corporation with its principal office or place of business at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act.

RESPONDENT’S BUSINESS PRACTICES

3. Google is a technology company best known for its web-based search engine, which provides free search results to consumers. Google also provides various free web products to consumers, including its widely used web-based email service, Gmail, which has been available since April 2004. Among other things, Gmail allows consumers to send and receive emails, chat with other users through Google’s instant messaging service, Google Chat, and store email messages, contact lists, and other information on Google’s servers.

4. Google’s free web products for consumers also include: Google Reader, which allows users to subscribe to, read, and share content online; Picasa, which allows users to edit, post, and share digital photos; and Blogger, Google’s weblog publishing tool that allows users to share text, photos, and video.

5. Google also offers consumers the ability to create a “Google profile,” which enables 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:

Complaint

- 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:

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

- 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:

When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use.

RESPONDENT'S LAUNCH OF GOOGLE BUZZ

7. On February 9, 2010, Google launched a social networking service called Google Buzz ("Google Buzz" or "Buzz") within the Gmail product. Google Buzz is a platform that allows users to share updates, comments, photos, videos, and other information through posts or "buzzes" made either publicly or privately to individuals or groups of users. Google used the information of consumers who signed up for Gmail, including first and last name and email contacts, to populate the social network. Without prior notice or the opportunity to consent, Gmail users were, in many instances, automatically set up with "followers" (people following the user). In addition, after enrolling in Buzz, Gmail users were automatically set up to "follow" other users.

8. On the day Buzz was launched, Gmail users who signed into their accounts were taken to a welcome screen that announced the new service and highlighted features such as: "No set up needed – You're already following the people you email

Complaint

and chat with the most in Gmail.” Gmail users had to elect one of two options to proceed to their inboxes: “Sweet! Check out Buzz” or “Nah, go to my inbox.” Exhibit A shows how the initial Buzz screen appeared to consumers.

- a. If a Gmail user selected “Nah, go to my inbox” from the initial Buzz screen, that user’s information was nonetheless shared in a number of ways:
 - i. The user could be “followed” by other Gmail users who had enrolled in Buzz.
 - ii. If the user had previously created a public Google profile, the user could appear on the public Google profiles of people who had enrolled in Buzz and were following the user.
 - iii. A Buzz link would appear in the list of links on the user’s Gmail page. If the user clicked on the that link, he or she would be taken to the Buzz welcome screen and automatically enrolled in Buzz, without any disclosure of that fact and without any further action on the user’s part. Exhibit B shows how the Buzz welcome screen appeared to consumers. The user would be enrolled in Buzz even if the user did not click the “Okay” button at the bottom of the welcome screen.
- b. Regardless of whether they chose “Sweet! Check out Buzz” or “Nah, go to my inbox,” Gmail users had an option to click a “Turn off Buzz” link, contained in small type at the bottom of the Gmail home page after login. Clicking that link removed the Buzz tab from the user’s Gmail page. Gmail users who had clicked “Sweet! Check out Buzz” or had clicked on the Buzz link in Gmail, then later clicked the “Turn off Buzz” link, nonetheless continued to appear as a “follower” on the Google profiles and Google Buzz pages of the people whom they emailed the most. In addition, on each such profile, a “follow” link was placed next to

Complaint

the Gmail user's name, so other individuals could begin following the user.

9. The setup process for Gmail users who enrolled in Buzz did not adequately communicate that certain previously private information would be shared publicly by default. Further, the controls that would allow the user to change the defaults were confusing and difficult to find.

- a. Users who clicked on "Sweet! Check out Buzz" from the Buzz welcome screen, as well as users that selected "Nah, go to my Inbox" and later clicked the Buzz tab, were directed to a Buzz welcome screen that stated: "You're set up to follow the people you email and chat with the most," and listed the users' followers and the people the user was set up to follow. However, there was no disclosure on this screen that, by default, those lists might later be posted on a user's public Google profile, exposing the list of people with whom a user chatted or emailed most often. See Exhibit B.
- 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

Complaint

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

Complaint

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)

Complaint

discontinued the feature that automatically connected to information from other websites, such as Picasa and Google Reader; and (7) fixed the @ reply function so that private email addresses of users would not be made public.

VIOLATIONS OF THE FTC ACT

13. As set forth in paragraph 6(a), respondent has represented, expressly or by implication, that it used, and would use, information from consumers signing up for Gmail only for the purpose of providing them with a web-based email service.

14. In truth and in fact, as described in paragraphs 7-11, respondent did not use information from consumers signing up for Gmail only for the purpose of providing them with a web-based email service. Instead, Google used this information to populate its new social 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

Complaint

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

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 (“Directive”). The Directive sets forth EU requirements for privacy and the protection of personal data. Among other things, it requires EU Member States to implement legislation that prohibits the transfer of personal data outside the EU, with exceptions, unless the European Commission (“EC”) has made a determination that the recipient jurisdiction’s laws ensure the protection of such personal data. This determination is commonly referred to as meeting the EU’s “adequacy” standard.

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.

Complaint

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 Privacy Principles of Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement, and is registered with

Complaint

the U.S. Department of Commerce's Safe Harbor Program.

25. In truth and in fact, as described in paragraph 7, respondent did not adhere to the US Safe Harbor Privacy Principles of Notice and Choice. In particular, respondent 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. Respondent 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. Therefore, the representations set forth in paragraphs 23 and 24 were, and are, false or misleading and constitutes a deceptive act or practice.

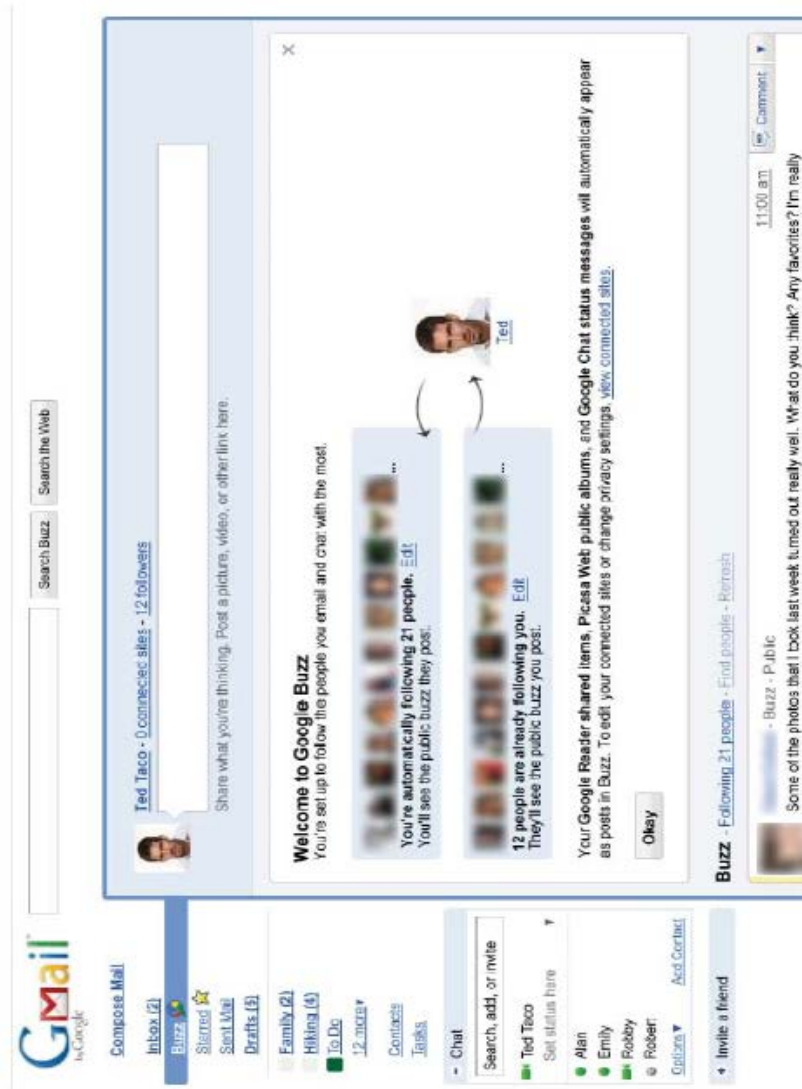
26. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this thirteenth day of October, 2011, has issued this complaint against respondent.

By the Commission.

Complaint

EXHIBIT B



Complaint

EXHIBIT C

How do you want to appear to others? ✕

Profile preview - [Edit](#)



Ted Taco
[Ted has 12 followers](#)
[Ted is following 19](#)

Your profile will include your name, photo, people you follow, and people who follow you.

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. [Why do I need a profile?](#)

Save profile and continue

[Cancel, don't post buzz](#)

Complaint

EXHIBIT D

How do you want to appear to others?

Profile preview - [Done editing](#)



Ted Taco

[Ted has 12 followers](#)
[Ted is following 19](#)

[Change](#)

Your profile includes your name, photo, people you follow, and people who follow you.

☒ **Show the lists of people I'm following and people following me on my profile**

View and edit the people you follow

[Unfollow](#)

[Unfollow](#)

[Unfollow](#)

[Unfollow](#)

[Unfollow](#)

[Unfollow](#)

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. [Why do I need a profile?](#)

Save profile and continue

[Cancel, don't post](#)

Decision and Order

DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft of Complaint which the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued, would charge the Respondent with violation of the Federal Trade Commission Act; and

The Respondent and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of the agreement is for settlement purposes only and does not constitute an admission by the Respondent that the law has been violated as alleged in such complaint, or that any of the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the Respondent has violated the Federal Trade Commission Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comments received from interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure prescribed in Section 2.34 of its Rules, 16 C.F.R. § 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following order:

1. Respondent Google is a Delaware corporation with its principal office or place of business at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

Decision and Order

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, “respondent” shall mean Google, its successors and assigns, officers, agents, representatives, and employees. For the purpose of Parts I, II, and III of this order, “respondent” shall also mean Google acting directly or through any corporation, subsidiary, division, website, or other device.
2. “Clear(ly) and prominent(ly)” shall mean:
 - a. In textual communications (e.g., printed publications or words displayed on the screen of a computer or mobile device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;
 - b. In communications disseminated orally or through audible means (e.g., radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;
 - c. In communications disseminated through video means (e.g., television or streaming video), the required disclosures are in writing in a form consistent with subpart (A) of this definition and shall appear on the screen for a duration sufficient

Decision and Order

for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication; and

- d. In all instances, the required disclosures: (1) are presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any other statements or disclosures provided by respondent.
3. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
4. “Google user” shall mean an identified individual from whom respondent has collected information for the purpose of providing access to respondent’s products and services.
5. “Covered information” shall mean information respondent collects from or about an individual, including, but not limited to, an individual’s: (a) first and last name; (b) home or other physical address, including street name and city or town; (c) email address or other online contact information, such as a user identifier or screen name; (d) persistent identifier, such as IP address; (e) telephone number, including home telephone number and mobile telephone number; (f) list of contacts; (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above.
6. “Third party” shall mean any individual or entity other than: (1) respondent; (2) a service provider of respondent that: (i) uses or receives covered information collected by or on behalf of respondent for and at the direction of the respondent and no other individual or entity, (ii) does not disclose the data, or any individually identifiable information derived from such data, to any individual or entity other than respondent, and (iii) does not use the data for any other purpose; or (3) any entity that uses covered

Decision and Order

information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, (ii) to enforce respondent's terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.

I.

IT IS ORDERED that respondent, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:

- A. the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to: (1) the purposes for which it collects and uses covered information, and (2) the extent to which consumers may exercise control over the collection, use, or disclosure of covered information.
- B. the extent to which respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any other entity, including, but not limited to, the U.S. EU Safe Harbor Framework.

II.

IT IS FURTHER ORDERED that respondent, prior to any new or additional sharing by respondent of the Google user's identified information with any third party, that: 1) is a change from stated sharing practices in effect at the time respondent collected such information, and 2) results from any change, addition, or enhancement to a product or service by respondent, in or affecting commerce, shall:

- A. Separate and apart from any final "end user license agreement," "privacy policy," "terms of use" page, or similar document, clearly and prominently disclose: (1) that the Google user's information will be

Decision and Order

disclosed to one or more third parties, (2) the identity or specific categories of such third parties, and (3) the purpose(s) for respondent's sharing; and

- B. Obtain express affirmative consent from the Google user to such sharing.

III.

IT IS FURTHER ORDERED that respondent, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, 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. Such program, the content and implementation of which must be documented in writing, shall contain privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information, including:

- A. the designation of an employee or employees to coordinate and be responsible for the privacy program.
- B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in the respondent's unauthorized collection, use, or disclosure of covered information, and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.
- C. the design and implementation of reasonable privacy controls and procedures to address the risks identified through the privacy risk assessment, and regular

Decision and Order

testing or monitoring of the effectiveness of those privacy controls and procedures.

- D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate privacy protections.
- E. the evaluation and adjustment of respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

IV.

IT IS FURTHER ORDERED that, in connection with its compliance with Part III of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons conducting such Assessments and preparing such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

Decision and Order

- A. set forth the specific privacy controls that respondent has implemented and maintained during the reporting period;
- B. explain how such privacy controls are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information;
- C. explain how the privacy controls that have been implemented meet or exceed the protections required by Part III of this order; and
- D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

V.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, unless respondent asserts a valid legal privilege, a print or electronic copy of:

- A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely disseminated statements that describe the extent to which respondent maintains and protects the

Decision and Order

privacy and confidentiality of any covered information, with all materials relied upon in making or disseminating such statements;

- B. for a period of six (6) months from the date received, all consumer complaints directed at respondent, or forwarded to respondent by a third party, that allege unauthorized collection, use, or disclosure of covered information and any responses to such complaints;
- C. for a period of five (5) years from the date received, any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
- D. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

VI.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

VII.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under

Decision and Order

this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. *Provided, however,* that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VIII.

IT IS FURTHER ORDERED that respondent shall, within ninety (90) days after the date of service of this order file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form in which respondent has complied with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, respondent shall submit additional true and accurate written reports.

IX.

This order will terminate on October 13, 2031, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

- A. any Part in this order that terminates in fewer than twenty (20) years;
- B. this order if such complaint is filed after the order has terminated pursuant to this Part.

Analysis to Aid Public Comment

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Google Inc. (“Google”).

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement’s proposed order.

On February 9, 2010, Google launched a social networking service called Google Buzz (“Google Buzz” or “Buzz”) within Gmail, its web-based email product. Google Buzz is a platform that allows users to share updates, comments, photos, videos, and other information through posts or “buzzes” made either publicly or privately to individuals or groups of users. Google used the information of consumers who signed up for Gmail, including first and last name and email contacts, to populate the social

Analysis to Aid Public Comment

network, which, in many instances, resulted in certain previously private information being made public.

The Commission's complaint 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. 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. The 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. Finally, the 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.

The proposed order contains provisions designed to prevent Google from engaging in the future in practices similar to those alleged in the complaint with respect to all Google products and services, not only Gmail or Buzz.

Part I of the proposed order prohibits Google from misrepresenting the privacy and confidentiality of any "covered information," as well as the company's compliance with any privacy, security, or other compliance program, including but not limited to the U.S.-EU Safe Harbor Framework. "Covered information" is defined broadly to include an individual's: (a) first and last name; (b) home or other physical address, including street name and city or town; (c) email address or other online contact information, such as a user identifier or screen name; (d) persistent identifier, such as IP address; (e) telephone number, including home telephone number and mobile telephone number; (f) list of contacts; (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above.

Analysis to Aid Public Comment

Part II of the proposed order requires Google to give Google users a clear and prominent notice and to obtain express affirmative consent prior to sharing the Google user's information with any third party in connection with a change, addition or enhancement to any product or service, where such sharing is contrary to stated sharing practices in effect at the time the Google user's information was collected. This provision is limited to users of Google's products and services whom Google has identified at the time it shares their information with third parties, for example, users who are logged into a Google product.

Part III of the proposed order requires Google to establish and maintain 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, and (2) protect the privacy and confidentiality of covered information.

The privacy program must be documented in writing and must contain privacy controls and procedures appropriate to Google's size and complexity, the nature and scope of its activities, and the sensitivity of covered information. Specifically, the order requires Google to:

- designate an employee or employees to coordinate and be responsible for the privacy program;
- identify reasonably-foreseeable, material risks, both internal and external, that could result in the unauthorized collection, use, or disclosure of covered information and assess the sufficiency of any safeguards in place to control these risks;
- design and implement reasonable privacy controls and procedures to control the risks identified through the privacy risk assessment and regularly test or monitor the effectiveness of the safeguards' key controls and procedures;
- develop and use reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from respondent, and require service providers by contract to

Analysis to Aid Public Comment

implement and maintain appropriate privacy protections;
and

- evaluate and adjust its privacy program in light of the results of the testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on the effectiveness of its privacy program.

Part IV of the proposed order requires that Google obtain within 180 days, and on a biennial basis thereafter for twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: it has in place a privacy program that provides protections that meet or exceed the protections required by Part III of the proposed order; and its privacy controls are operating with sufficient effectiveness to provide reasonable assurance that the privacy of covered information is protected.

Parts V through IX of the proposed order are reporting and compliance provisions. Part V requires that Google retain all “widely disseminated statements” that describe the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, along with all materials relied upon in making or disseminating such statements, for a period of three (3) years. Part V further requires Google to retain, for a period of six (6) months from the date received, all consumer complaints directed at Google, or forwarded to Google by a third party, that allege unauthorized collection, use, or disclosure of covered information and any responses to such complaints. Part V also requires Google to retain for a period of five (5) years from the date received, documents that contradict, qualify, or call into question its compliance with the proposed order. Finally, Part V requires that Google retain all materials relied upon to prepare the third-party assessments for a period of three (3) years after the date that each assessment is prepared.

Part VI requires dissemination of the order now and in the future to principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having

Concurring Statement

supervisory responsibilities relating to the subject matter of the order. Part VII ensures notification to the FTC of changes in corporate status. Part VIII mandates that Google submit an initial compliance report to the FTC and make available to the FTC subsequent reports. Part IX is a provision “sunsetting” the order after twenty (20) years, with certain exceptions.

The purpose of the analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed order or to modify its terms in any way.

**CONCURRING STATEMENT OF
COMMISSIONER J. THOMAS ROSCH**

I concur in accepting, subject to final approval, a consent agreement from Google Inc. (“Google”) for public comment. However, it should be emphasized that this consent agreement is being accepted, subject to final approval. I have substantial reservations about Part II of the consent agreement. My concerns are threefold. Before I describe them, however, I want to make clear that I do not mean to defend Google. Google can – and should – speak for itself. However, I believe that, as a Commission, we must always be concerned that a consent agreement, like a litigated decree, is consistent with the public interest. For that reason, I am opposed to accepting consent agreements that may be contrary to the public interest because a party is willing to agree to terms that hurt other competitors as much or more than the terms will hurt that party. That may occur, for example, when a consent agreement is used as “leverage” in dealing with the practices of other competitors. Part II of the proposed consent order may be susceptible to this happening.

Concurring Statement

More specifically, the crux of the violation alleged in the Complaint is that Google represented in its general “Privacy Policy” that “When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different from the purpose for which it was collected, then we will ask for your consent prior to such use.” However, when Google initiated its social networking service (“Google Buzz”) it used personal information previously collected for other purposes without asking for users’ consent prior to this use. Part II of the proposed consent order prohibits Google, without prior “express affirmative consent” (an “opt-in” requirement) from engaging in any “new or additional sharing” of previously collected personal information “with any third party” that results from “any change, addition, or enhancement” to any Google product or service.

First, Google did not represent in its general “Privacy Policy” (or otherwise, according to the Complaint) that the “consent” it would seek would require consumers to “opt in” as required by Part II. Indeed, the Complaint does not allege that Google ever asked consumers to signify their “consent” by “opting in” (as opposed to “opting out”). To be sure, insofar as Google did not seek “consent” at all, its representation in its general “Privacy Policy” was deceptive in violation of Section 5. But the “opt in” requirement in Part II is seemingly brand new. It does not echo what Google promised to do at the outset. In the separate Statement that I issued when the staff issued its preliminary Privacy Report, I expressed concern about whether an “opt in” requirement in these circumstances might sometimes be contrary to the public interest. Then, as now, I was concerned that it might be used as leverage in consent negotiations with other competitors.

Second, Part II of the proposed consent order applies whenever Google engages in any “new or additional sharing” of previously collected personal information “with any third party” for the next twenty years, not just any “material” new or additional sharing of that information. Because internet business models (and technology) change so rapidly, Google (and its competitors) are bound to engage in “new or additional” sharing of previously collected information with third parties during that

Concurring Statement

period. That means that Part II is certain to apply (and with some frequency) during that period as long as Google does not warn users or consumers in its “general Privacy Policy” that it may engage in such sharing in the future.

Third, Part II applies not just to Google’s social networking services or products, but to every single Google service or product that undergoes some “change, addition, or enhancement” (terms that are not defined in Part II) that results from the sharing of certain information. As a practical matter, this means that Google is at risk that Part II will apply across the board to every existing product or service that Google offers, including any product or service that involves the tracking and sharing of identified Google users’ browsing behavior.

In short, on the face of it, Part II seems to be contrary to Google’s self-interest. I therefore ask myself if Google willingly agreed to it, and if so, why it did so. Surely it did not do so simply to save itself litigation expense. But did it do so because it was being challenged by other government agencies and it wanted to “get the Commission off its back”? Or did it do so in hopes that Part II would be used as leverage in future government challenges to the practices of its competitors? In my judgment, neither of the latter explanations is consistent with the public interest.

Nor am I comforted that the purpose and effect of Part II may be to “fence in” Google. I am aware of the teaching of *Jacob Siegel Co. v. FTC*, 327 U.S. 608 (1946) that a “fencing in” order may cover legal conduct as long as that conduct is “reasonably related” to the violation. Even if Part II may be considered to cover conduct that is “reasonably related” to the violation here, any consent order, whether litigated or negotiated, must be consistent with the public interest. I look forward to public comment about whether Part II of the proposed consent order meets that requirement.

Complaint

IN THE MATTER OF

**KOBY BROWN AND GREGORY PEARSON
DOING BUSINESS AS DERMAPPS**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECS. 5(A) AND 12 OF THE FEDERAL TRADE COMMISSION ACT

*Docket No. C-4337; File No. 102 3205
Filed, October 13, 2011 — Decision, October 13, 2011*

This consent order addresses allegations that Koby Brown and Gregory W. Pearson, doing business as DERMAPPS (“Respondents”), violated the FTC Act by misrepresenting the effectiveness of its AcneApp mobile software application. The complaint alleges that Respondents falsely claimed its AcneApp mobile software application effectively treated acne, by holding light-emitting display screen next to the area of skin to be treated for several minutes each day. The complaint alleges Respondents falsely represented a journal study proved that red and blue light therapy was an effective treatment for acne. The order prohibits Respondents from making any representation that AcneApp or any other device provides effective treatment for acne, unless Respondents have competent and reliable scientific evidence to substantiate the claim. The order further requires Respondents to pay approximately \$15,000 towards consumer relief.

Participants

For the *Commission*: Stacey Ferguson and James A. Prunty.

For the *Respondents*: Sesha Kalapatapu.

COMPLAINT

The Federal Trade Commission, having reason to believe that Koby Brown and Gregory W. Pearson (“respondents”), individually and doing business as DERMAPPS, have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Koby Brown (“Brown”) is the developer, and a seller or marketer, of a mobile software application called “AcneApp.” At all times relevant to this complaint, Brown,