GARDY & NOTIS, LLP
Mark C. Gardy
James S. Notis *(pro hac vice)*
Kelly A. Noto *(pro hac vice)*
Charles A. Germershausen
560 Sylvan Avenue
Englewood Cliffs, New Jersey 07632
Tel: 201-567-7377
Fax: 201-567-7337

GRANT & EISENHOFER P.A.
James J. Sabella *(pro hac vice)*
Diane Zilka *(pro hac vice)*
Kyle McGee *(pro hac vice)*
485 Lexington Avenue, 29th Floor
New York, New York 10017
Tel: 646-722-8500
Fax: 646-722-8501

BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
Sarah N. Westcot (State Bar No. 264916)
1990 North California Boulevard, Suite 940
Walnut Creek, California 94596
Tel: 925-300-4455
Fax: 925-407-2700

Interim Lead Counsel for the Class

[Additional counsel listed on signature page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE GOOGLE, INC. PRIVACY POLICY LITIGATION	CASE NO. 12-CV-01382 PSG **CONSOLIDATED FIRST AMENDED CLASS ACTION COMPLAINT** **COMPLAINT FOR DAMAGES, EQUITABLE, AND INJUNCTIVE RELIEF** **DEMAND FOR JURY TRIAL**

Plaintiffs Pedro Marti, David Nisenbaum, Robert B. DeMars, Lorena Barrios, Nicholas Anderson, Matthew Villani, and Scott McCullough ("Plaintiffs"), by and through their attorneys, bring this class action complaint on their own behalf and on behalf of all others similarly situated, to obtain an injunction, damages, costs of suit, and attorneys' fees from defendant Google, Inc. ("Google"). Plaintiffs complain and allege, upon knowledge as to themselves and their acts, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This is a nationwide class action against Google on behalf of all persons and entities in the United States that acquired a Google account between August 19, 2004 and February 29, 2012, and continued to maintain that Google account on or after March 1, 2012, when Google's new privacy policy went into effect.

2. Google is a technology and advertising company that provides free web-based products to billions of consumers across the globe. Over one billion consumers use Google's search engine, google.com, each week; over 425 million consumers use Google's web-based email service, Gmail; and Google's video sharing site, YouTube, streams over 4 billion videos per day to consumers.

3. Google can offer these important, globally pervasive products free of charge to consumers due to its primary business model – advertising. In 2011, Google's revenues were $37.91 billion, approximately 95% of which ($36.53 billion) came from advertising. In 2012, Google's revenues increased to $46.04 billion, approximately 95% of which ($43.69 billion) came from advertising.

4. Google's advertising revenues are dependent upon its ability to deliver highly relevant, targeted advertisements that are tailored to a consumer's interests and online habits. In order to accomplish this, Google logs personal identifying information, browsing habits, search queries, responsiveness to ads, demographic information, declared preferences, and other information about each consumer that uses its products. Google's Gmail service also scans and discloses to other Google services the contents of Gmail communications. Google uses this

information, including the contents of Gmail communications, to place advertisements that are tailored to each consumer while the consumer is using any Google product or browsing third-party sites that have partnered with Google to serve targeted ads.

5. Prior to March 1, 2012, information collected in one Google product was not commingled with information collected during the consumer's use of other Google products. Thus, Google did not, for instance, previously associate a consumer's Gmail account (and therefore his or her name and identity, his or her private contact list, or the contents of his or her communications) with the consumer's Google search queries or the consumer's use of other Google products, like YouTube, Picasa, Voice, Google+, Maps, Docs, and Reader.

6. Indeed, Google previously maintained a separate privacy policy for each of its products, all of which confirmed that Google would use the consumer's personal information strictly in order to provide that particular product or service to the consumer, and that Google would not use it for any other purpose without the consumer's explicit consent.

7. On March 1, 2012, however, Google eliminated the majority of its separate privacy policies and created one, universal privacy policy that enabled Google to cross-pollinate consumers' personal information, including the contents of electronic communications in Gmail, across Google products, despite prior representations that Google would not use that information for any purpose other than to provide that specific service to the consumer. As stated by Google:

> Our new Privacy Policy makes clear that, if you're signed in, we may combine information you've provided from one service with information from other services. In short, we'll treat you as a single user across all our products, which will mean a simpler, more intuitive Google experience.

8. But this "simpler, more intuitive Google experience" comes at a tremendous cost to the privacy interests and the legal rights of Google's users, as explained in more detail herein. Following Google's introduction of the unified privacy policy, Google now uses detailed and highly specific personal information gathered from multiple product platforms, including the contents of a consumer's Gmail communications, to optimize search results and, thus, Google's ability to display targeted ads when that consumer uses the google.com search engine or other Google products that

employ querying, or when that consumer visits third-party sites that have partnered with Google in its advertising networks.

9. The new privacy policy thus commingles user data without consumers' consent, and it no longer allows consumers to keep the personal information and communications contained on one Google service separate from information gathered about the consumer by other Google services. By implementing the new privacy policy, Google violated its prior privacy policies and rendered them misleading because they stated that Google would not utilize information provided by a consumer in connection with his or her use of one product, with any other product, for any reason, without the consumer's explicit consent.

10. Google's new privacy policy also violates consumers' privacy rights, because it allows Google to take information from a consumer's Gmail account, for instance, which may have one (higher) expectation of privacy, and use it in a different context, such as to personalize results from the Google search engine, or to personalize advertisements viewed while the consumer is surfing the internet, practices with respect to which a consumer has an entirely different (lower) expectation of privacy. It thus provides to those services with different kinds of information that they were not originally intended to have access to. Moreover, this cross-pollination is achieved through independent third party entities that "process" and are thus exposed to users' personal information, including the contents of their Gmail communications.

11. Similar cross-referencing of billions of consumers' personal information previously resulted in an October 13, 2011 Consent Order with the Federal Trade Commission ("FTC"), in which the FTC found that Google deceptively claimed it would seek the consent of consumers before using their information for a purpose other than for which it was collected, and that Google had misrepresented consumers' ability to exercise control over their information. In announcing the Consent Order, Jon Leibowitz, Chairman of the FTC, stated, "when companies make privacy pledges, they need to honor them."

12. Google's products and services have become a staple of society, and billions of consumers across the globe are affected by Google's new privacy policy. On February 22, 2012,

thirty-six Attorneys General wrote in an open letter stating, "This invasion of privacy will be costly for many users to escape. For users who rely on Google products for their business – a use that Google has actively promoted – avoiding this information sharing may mean moving their entire business over to different platforms, reprinting any business cards or letterhead that contained Gmail addresses, re-training employees on web-based sharing and calendar services, and more."

13. Google's display advertising revenue is second in the United States only to Facebook. Facebook garners a larger market share of display advertising revenue because consumers that use Facebook set up, manage, maintain, and populate personal profiles with very specific information about themselves. This allows Facebook to deploy a more complete picture of the individual to most effectively target advertisers' messages only to qualified consumers, providing advertisers the best return on their investments, using information each consumer willingly supplies to Facebook.

14. Unlike Facebook, a holistic view of each consumer was previously unavailable to Google. Before implementing the new privacy policy, Google could not easily target consumers for advertising because Google used bits and pieces of anonymous information garnered from each discrete Google service, which had more than 60 distinct privacy policies.

15. Thus, Google's new privacy policy is nothing more than Google's effort to garner a larger market share of advertising revenue by offering targeted advertising capabilities that compete with or surpass those offered by social networks, such as Facebook, where all of a consumer's personal information is available in one site.

16. Google is not only capable of serving targeted advertisements that draw on a user's histories on various, previously segregated platforms, but it can even notify users that other Google users with whom they have interacted (for instance, a Gmail contact) have stated a preference for a product, brand, ad, or website. The users that have stated such a preference are not compensated for Google's use of that preference as an endorsement to other users known (thanks to Google's new cross-platform data sharing practice) to communicate with the endorser. Google, however, extracts a profit by attracting more advertisers, given the strong persuasive power of the endorsement of friends and contacts.

17. As explained in more detail below, in serving such personalized endorsements, Google appropriates the names, faces, and/or other aspects of a user's likeness by incorporating them into a graphic representation indicating that a friend or contact of the user has clicked "+1" – a device similar to Facebook's "Like" function – in connection with a given ad, brand, product, or website. For example, Plaintiff Marti's name, face, and/or likeness was appropriated by Google and used in graphical "+1" advertisements created by Google, without Plaintiff Marti's consent and without compensation.

18. Although the Facebook "Like" feature is objectionable on basic privacy grounds and should under no circumstances constitute a model for other advertising companies to mimic, it is important to note that the profiles on Facebook are created, populated, and managed by the consumers themselves, and the consumers have some measure of control over the personal information appended to their Facebook profiles. Google's conduct is even more objectionable, therefore, because *Google* creates, populates, and manages the profiles of its users. Thus, a consumer's expectation of privacy on Facebook is much different than his or her expectation of privacy when using Google products, where Google collects and aggregates information about the consumer without the consumer's consent, and which likely includes information that the individual would keep private, and choose not to post, even on Facebook.

19. Users of Google's immensely popular Android mobile operating system – which is pre-loaded on millions of devices including smartphones, tablets, digital assistants, and similar devices – have suffered similar violations of their privacy interests and other injuries, as explained in more detail below. Google requires that users of Android devices create an account to access Google Play (formerly known as the Android Market), which is the primary service through which Android users purchase or otherwise acquire apps for their devices. Once such an account is created, the Android user is *permanently* "logged in" so that each and every action taken on the device is recorded and aggregated with that user's other Google accounts, including their Gmail, YouTube, Picasa, Google+, Maps, Docs, and other accounts. There is no way to opt out of this practice, and many users have voiced their disapproval of Google's treatment of Android users in this regard. For

example, Plaintiff Nisenbaum owned and used an Android device before and after March 1, 2012, but subsequently ceased using the device and acquired an Apple device in its place in substantial part because of Google's invasive practices. Switching from an Android device to another comparable device is costly to consumers. That burden should be borne by Google rather than consumers.

20. To make matters worse, Google subjects Android device users to yet another injury by secretly disclosing to third-party application developers certain sensitive personal information of users that download applications through Google Play, without such users' authorization or consent. Indeed, Google causes this disclosure to occur automatically and without even notifying Android users that it is occurring, each and every time they download and/or purchase an Android application through Google Play. The disclosed information includes at least the name, email address, and physical or geographical location associated with the Play account and/or device. This unauthorized disclosure subjects every affected Android app user to a substantially increased, unexpected, and unreasonable risk of further interception or dissemination of their personal information as well as of harassment and even identity theft.

21. Further, Android device users are made to carry the burden of involuntarily transmitting this additional data to third parties, in the form of depleted device battery power and extra bandwidth consumed by the device. As courts have recognized, device battery power and bandwidth are not free but must be paid for by individual users. All Android device users that have downloaded at least one application through Google Play have therefore been injured in a measurable and quantifiable manner by Google's practice of requiring the disclosure of certain personal information of those users to third parties, in contravention of Google's privacy policy.

22. Accordingly, contrary to Google's previous privacy policies and contrary to Plaintiffs' and other users' agreements with Google at the time their accounts were created, Google is now aggregating such users' personal information without their explicit consent; is disclosing the contents of users' Gmail communications to other services and products as well as independent third parties for advertising purposes; is aggressively appropriating the likenesses of many of its users for advertising purposes; is driving Android device users to switch to non-Android devices because of

these invasions of user privacy interests; is disclosing certain personal information of Android device users to third-party application developers, subjecting such users to heightened and unexpected risks as well as consuming additional battery power and bandwidth in the process; and has failed to provide a simple, effective opt-out mechanism by which these harms can be avoided. Consumers are entitled to damages and injunctive relief as a result.

JURISDICTION AND VENUE

23. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises under federal statutes, namely the Federal Wiretap Act, 18 U.S.C. § 2511, and the Stored Communication Act, 18 U.S.C. § 2701. This Court has jurisdiction over the remaining claims pursuant to 28 U.S.C. § 1367. Furthermore, this Court has jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because the aggregated claims of the individual Class members exceed the sum or value of $5,000,000, exclusive of interests and costs, and this is a class action in which more than two-thirds of the proposed plaintiff Class, on the one hand, and defendant Google, on the other, are citizens of different states.

24. This Court has jurisdiction over Google because it maintains its principal headquarters in California; is registered to conduct business in California; has sufficient minimum contacts in California; or otherwise intentionally avails itself of the markets within California through the promotion, sale, marketing, and distribution of its products and services to render the exercise of jurisdiction by this Court proper and necessary. Moreover, Google's wrongful conduct (as described herein) emanates from California and foreseeably affects consumers in California. Most, if not all, of the events complained of below occurred in or emanated from Google's corporate headquarters located in Mountain View, California.

25. Venue is proper in this District under 28 U.S.C. § 1391(a) because Google resides in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

26. Venue is also proper in this Court because Google's User Agreement provides:

> The laws of California, U.S.A., excluding California's conflict of laws rules, will apply to any disputes arising out of or relating to these terms or the Services. All

1 claims arising out of or relating to these terms or the Services will be litigated
2 exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts.

3 *Available at* http://www.google.com/intl/en/policies/terms/.

4 **THE PARTIES**

5 27. Plaintiff Pedro Marti ("Marti") is a New York resident. Marti acquired his Gmail
6 account on September 14, 2004, and a Google+ account in 2011, and continued to maintain his
7 Gmail and Google+ accounts on March 1, 2012. Like all members of the Class, Google aggregated
8 Marti's personal information without his consent. Furthermore, as alleged more fully below, Google
9 has used Plaintiff Marti's likeness, including his name and face, in display advertisements without
10 his authorization and without compensating him. Plaintiff Marti purchased an HTC G2, an Android-
11 powered mobile device, in or about January of 2011, and continued to use it on or after March 1,
12 2012, and uses it still. Plaintiff Marti has downloaded at least one Android application through
13 Google Play.

14 28. Plaintiff David Nisenbaum ("Nisenbaum") is a New York resident. Nisenbaum
15 acquired his Gmail account in or about June of 2010, and continued to maintain his Gmail account
16 on March 1, 2012. Like all members of the Class, Google aggregated Nisenbaum's personal
17 information without his consent. Furthermore, Plaintiff Nisenbaum purchased an Android-powered
18 HTC mobile device in or about June 2010 and continued to own and use that mobile device on or
19 after March 1, 2012. Like all Android device users, Plaintiff Nisenbaum could not prevent Google's
20 aggregation of his personal information without purchasing a new mobile device that is not powered
21 by Android. In or about May 2012, Plaintiff Nisenbaum ceased using his Android device and
22 purchased an alternative mobile device that was not powered by Android, in substantial part because
23 of his concern for the privacy of his personal information, including his communications.

24 29. Plaintiff Robert B. DeMars ("DeMars") is a California resident. DeMars acquired his
25 Gmail account in or about May of 2011, and continued to maintain his Gmail account on March 1,
26 2012. Like all members of the Class, Google aggregated DeMars' personal information without his
27 consent. Plaintiff DeMars purchased an LG Optimus, an Android-powered mobile device, in or
28

about May of 2011, and continued to use it on or after March 1, 2012. Plaintiff DeMars purchased a Samsung Galaxy II, another Android-powered mobile device, thereafter, and uses it at present. Plaintiff DeMars has downloaded at least one Android application through Google Play, on both his LG Optimus and his Samsung Galaxy II.

30. Plaintiff Lorena Barrios ("Barrios") is a California resident. Barrios acquired her Gmail account in or about February of 2012, and continued to maintain her Gmail account on March 1, 2012. Like all members of the Class, Google aggregated Barrios' personal information without her consent. Plaintiff Barrios purchased a Verizon HTC mobile device powered by Android in or about February of 2012, and continued to use it on or after March 1, 2012, and uses it still. Plaintiff Barrios has downloaded at least one Android application through Google Play.

31. Plaintiff Nicholas Anderson ("Anderson") is a California resident. Anderson acquired his Gmail account in or about June of 2005, and continued to maintain his Gmail account on March 1, 2012. Like all members of the Class, Google aggregated Anderson's personal information without his consent. Plaintiff Anderson purchased a Samsung Nexus S, an Android-powered mobile device, in or about May of 2011, and continued to own that mobile device on or after March 1, 2012, and uses it still. Plaintiff Anderson has downloaded at least one Android application through Google Play.

32. Plaintiff Matthew Villani ("Villani") is a New Jersey resident. Villani acquired his Gmail account in 2007, and continued to maintain his Gmail account on March 1, 2012. Like all members of the Class, Google aggregated Villani's personal information without his consent. Plaintiff Villani purchased a Droid X, an Android-powered mobile device, in or about September of 2010, and continued to own that mobile device on or after March 1, 2012, and uses it still. Plaintiff Villani has downloaded at least one Android application through Google Play.

33. Plaintiff Scott McCullough ("McCullough") is a New Jersey resident. McCullough acquired his Gmail account in 2011, and continued to maintain his Gmail account on March 1, 2012. Like all members of the Class, Google aggregated McCullough's personal information without his consent. Plaintiff McCullough purchased a Casio G'zOne Commando, an Android-powered mobile

device, in or about July of 2011, and continued to own that mobile device on or after March 1, 2012, and uses it still. Plaintiff McCullough has downloaded at least one Android application through Google Play.

34. Google is a Delaware corporation with its principal place of business located at 1600 Amphitheatre Parkway, Mountain View, California 94043. At all times relevant hereto, Google was a multinational, publicly held internet technologies corporation. Google owns, services, and develops internet-based services and products. Google was first incorporated as a privately held company on September 4, 1998, with its initial public offering to follow on August 19, 2004. Google consumers do not pay money to use Google's services and products. Instead, Google's primary business model is advertising, which constituted over 95% of Google's profits last year.

PLAINTIFFS' CLASS ALLEGATIONS

35. Plaintiffs seek to bring this case as a nationwide class action on behalf of themselves and all others similarly situated in the United States as members of the proposed Class, defined as follows:

> All persons and entities in the United States that created any Google account between August 19, 2004 and February 29, 2012, and continued to maintain that Google account on or after March 1, 2012.

36. Plaintiffs also seek to represent a nationwide subclass of individuals situated similarly to Plaintiff Nisenbaum (the "Android Device Switch Subclass"), defined as follows:

> All persons and entities in the United States that acquired a device powered by Android between August 19, 2004 and February 29, 2012, continued to own that device on or after March 1, 2012, and switched to a non-Android device on or after March 1, 2012.

37. Plaintiffs also seek to represent a nationwide subclass of individuals situated similarly to Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough (the "Android App Disclosure Subclass"), defined as follows:

> All persons and entities in the United States that acquired a device powered by Android between August 19, 2004 and the present, and downloaded at least one Android application through Google Play.

38. Excluded from the Class, the Android Device Switch Subclass, and the Android App Disclosure Subclass are all claims for wrongful death, survivorship and/or personal injury by Class, Android Device Switch Subclass, or Android App Disclosure Subclass members. Also excluded from the Class, Android Device Switch Subclass, and Android App Disclosure Subclass is Google, any entity in which Google has a controlling interest, and its legal representatives and successors.

NUMEROSITY

39. The Class is so numerous that joinder of all of its members is impractical. Upon information and belief, Google has provided products and services to millions of consumers in the United States, and there are millions of devices powered by Android.

40. Although the precise number of Class and Subclass members and their addresses and/or email addresses is unknown to Plaintiffs, that information is readily ascertainable from Google's records. Class and Subclass members may be notified on the pendency of this action by mail, email, or internet publication, supplemented (if deemed necessary or appropriate by the Court) by published notice.

COMMON QUESTIONS OF LAW AND FACT

41. Common questions of law and fact exist as to all Class and Subclass members. These questions predominate over questions affecting only individual Class and Subclass members. These common legal and factual questions include but are not limited to the following:

a. Whether Google deceptively claimed that it would seek the consent of consumers before using their personal information for a purpose other than that for which it was collected, in breach of its contracts with its users;

b. Whether Google misrepresented the ability of consumers to exercise control over their personal information, in breach of its contracts with its users;

c. Whether Google's new privacy policy deceptively claims that it does not sell personal information to advertisers when advertisers can, and in fact do, purchase targeting services from Google that use the consumer's personal information, and Google profits as a result, in breach of its contracts with its users;

1 d. Whether Google's practice of sharing users' personal information, including the
2 contents of users' electronic communications, that was provided to one service or product (such as
3 Gmail) with different services or products (such as google.com search, Picasa, YouTube, Voice,
4 Google+, etc.) constitutes a violation of federal privacy statutes;
5 e. Whether the fact that independent third party entities are used by Google to cross-
6 pollinate users' personal information across multiple services or products constitutes a violation of
7 federal privacy statutes;
8 f. Whether Google's unauthorized and uncompensated use of users' names, faces, and
9 other aspects of their likenesses in display advertisements endorsing brands or products that partner
10 with Google constitutes a violation of common law and state statutory privacy rules;
11 g. Whether Google violated its previous privacy policy by merging data across products
12 and services without consumers' explicit consent, in breach of its contracts with its users;
13 h. Whether Google's opt-out practices for its new privacy policy are deceptive and
14 misleading;
15 i. Whether consumers can effectively opt out of Google's new privacy policy;
16 j. Whether Android users can effectively opt out of Google's new privacy policy;
17 k. Whether Google should provide an opt-in measure for its new privacy policy;
18 l. Whether Plaintiffs and the Class, Android Device Switch Subclass, and Android App
19 Disclosure Subclass are entitled to injunctive relief;
20 m. Whether Android Device Switch Subclass members are entitled to the cost of
21 purchasing a new, non-Android powered device;
22 n. Whether Android App Disclosure Subclass members are entitled to remuneration for
23 their losses associated with device battery power and bandwidth consumed without their
24 authorization in transmitting certain personal information to third-party application developers; and
25 o. Whether Plaintiffs and the Class, the Android Device Switch Subclass, and the
26 Android App Disclosure Subclass are entitled to damages, costs of suit, and attorneys' fees.
27
28

TYPICALITY

42. Plaintiffs' claims are typical of the claims of the Class and Subclass. Plaintiffs and each member of the proposed Class created one or more Google accounts between August 19, 2004 and February 29, 2012, and continued to maintain those Google accounts after March 1, 2012; each member of the Android Device Switch Subclass acquired a device powered by Android between August 19, 2004 and February 29, 2012, continued to own that device on or after March 1, 2012, and acquired an alternative, non-Android device on or after March 1, 2012; and each member of the Android App Disclosure Subclass downloaded at least one Android application through Google Play on an Android device between August 19, 2004 and the present.

43. In connection with their respective use of Google products, Plaintiffs and each Class and Subclass member were subject to the same disclosures and agreed to the same privacy policy or terms and conditions existing at the time they began using Google products.

44. Google has used Plaintiffs' and all Class and Subclass members' personal information without their consent (and, where a Plaintiff's likeness was used by Google in advertisements, without compensation), inconsistent with Google's affirmative representations, and to Google's financial benefit. Plaintiffs and all Class and Subclass members have suffered injuries as set forth below in the section titled, "Plaintiffs' Injuries Resulting from Google's Privacy Overhaul," and sustained damages as a result, including losses directly caused by Google's actions as alleged herein.

ADEQUACY OF REPRESENTATION

45. Plaintiffs can and will fairly and adequately represent and protect the interests of the Class and Subclasses, and have no interests that conflict with or are antagonistic to the interests of the Class and Subclasses. Plaintiffs have retained attorneys competent and experienced in class action litigation.

SUPERIORITY

46. A class action is superior to any other available method for the fair and efficient adjudication of this controversy, since, as demonstrated above, common questions of law and fact overwhelmingly predominate over any individual questions that may arise.

47. The prosecution of separate actions by individual members of the Class and Subclasses would create a risk of inconsistent or varying adjudications with respect to individual members of the Class which would establish incompatible standards of conduct for Google, or adjudication with respect to individual members of the Class and Subclasses which would, as a practical matter, be dispositive of other members not parties to the adjudications or substantially impair or impede their ability to protect their interests.

48. Google has acted or refused to act on grounds generally applicable to all Class and Subclass members, thereby making appropriate any final judgment with respect to the Class and Subclasses as a whole.

SUBSTANTIVE ALLEGATIONS

Google's Business Model

A. General Background

49. Google is a technology and advertising company that provides free web products to consumers. Google's products are globally pervasive and have become staples of society.

50. Although Google does not charge consumers to use its many products, Google's revenues are staggeringly high. The company produces revenue primarily by selling advertising to other businesses. In 2011, Google's revenues were $37.91 billion, approximately 95% of which ($36.53 billion) came from advertising. In 2012, Google's revenues increased to $46.04 billion, approximately 95% of which ($43.69 billion) came from advertising.

51. Before Google's implementation on March 1, 2012 of the new privacy policy, each Google product was governed by a separate privacy policy that described the permissible uses to which Google may put personal information collected during the use of each specific product.

Google also maintained a general privacy policy that provided default terms, from which individual product policies could deviate.

52. Because its products generate substantial web traffic, the ads Google is paid to host are valuable to advertisers. Although competitors, such as Microsoft and Yahoo!, offer similar ad placement within most of their products (such as bing.com or yahoo.com), Google remains the most popular – and most profitable – purveyor of search-related ads.

53. To maintain its industry position, Google is constantly enhancing its ability to target relevant ads to precisely those consumers most likely to make a purchase from the advertiser.

B. Google.com

54. Google's well-known and globally utilized search engine is google.com. It dominates the search engine industry, representing over 65% of Internet searches in the United States. Over one billion consumers use google.com each week. According to Alexa, a web statistics company, google.com is the most heavily-trafficked website on the Internet.

55. A consumer must set up a Google account to use many of Google's products. On all google.com searches, users will see targeted ads at the top and side of their search results. If the user is not signed in to any Google account while making the search, Google displays ads related to the terms searched; if the user is signed in to a Google account, Google draws not only on the terms searched but also on the user's history of google.com searches and activity on other Google products to determine which ads are most likely to generate a sale for the advertiser, and displays those ads.

C. Gmail

56. Gmail is Google's widely used web-based email service that has been available since 2004. It allows consumers to send and receive emails, chat with other consumers through Google Chat (Google's instant messaging service), and stores consumers' email messages, contact lists, calendar entries, and other information on Google's servers. When viewing a message on Gmail, targeted advertisements appear at the top and side of each message. The ads that appear while viewing a mailbox on Gmail, rather than a specific message, are determined with reference to the content of the mailbox being viewed. The ads that appear while viewing a message on Gmail are

determined with reference to the content of the specific email message being viewed. Gmail scans the contents of all messages to determine which ads to display.

57. Through the use of certain computer systems, applications, and/or code that are unrelated to the provision of the Gmail service, Google exports portions of users' personal information from Gmail, including the contents and/or data derived from the contents of users' Gmail communications, for use in other Google products and for use in advertising on third-party sites that have partnered with Google in advertising networks.

58. This cross-pollination is achieved through independent third party entities that "process" and are thus exposed to users' personal information, including the contents of their Gmail communications. The Gmail platform has in place an automatic mechanism that routes incoming and outgoing messages contemporaneously to such third parties – not, or not only, to facilitate the transmission of such messages, but to distribute portions or derivations of the contents of Gmail communications to other Google services for use in those other services and in advertising on third-party websites that have partnered with Google in advertising networks.

D. Google+

59. Google+ is Google's web-based social network where a consumer can set up a personal profile and share photos, links, videos and text with friends. It was intended by Google to compete with Facebook. However, Google+ is not as widely used by consumers and is less popular than Facebook. Google claims that Google+ had 500 million users, of which approximately 235 million were "active," as of December 2012 (Facebook claims to have over one billion active users). Users must provide their real name and gender when signing up. Google suspends accounts that use pseudonyms. Like other Google products, targeted advertisements appear across Google+. As explained in more detail below, Google+ thrives on the "+1" concept, by which Google+ users could indicate that they liked a particular website, ad, product, or brand. Google then serves targeted ads to different users indicating that others they know have declared a preference for that website, ad, product, or brand by clicking "+1."

60. Recent market research suggests that Google+ is rapidly growing thanks to Google's integration of its many privacy policies and its new practice of linking product platforms. According to a report issued on January 22, 2013 by GlobalWebIndex, a digital market research organization, Google+ has approximately 343 million active users. This finding places Google+ ahead of major social networking and microblogging services like Twitter and LinkedIn, and behind only Facebook. As GlobalWebIndex reports (in commentary, January 28, 2013), "[T]he social media landscape is becoming an oligopoly with the big 3 (Facebook, Google and Twitter) dominating on a global scale due to their level of integration throughout the web. This is a fundamental reason why Google+ has been so quick to grow. *It links together and increasingly enhances all of Google's other products from Android to Gmail to Search in a way that builds a complete digital experience for the user and works as a social layer, not just a network.*"

61. According to GlobalWebIndex, more than 40% of Google+ users have clicked "+1" for at least one product, brand, ad, or website in the 18 months preceding January 2013.

E. YouTube

62. YouTube is a video sharing site that Google purchased in 2006, where consumers can stream videos of interest to them. According to Alexa, YouTube is the third most heavily-trafficked website on the Internet. YouTube serves over 4 billion videos to consumers per day. Like other Google products, targeted advertisements appear across YouTube.

63. According to GlobalWebIndex's recent research, YouTube is the third most popular social networking site on the internet, after Facebook and Google+.

F. Maps

64. Google Maps allows consumers to view satellite images of locations all over the world, plan routes for traveling by foot, car, or public transport, and has a GPS-like service that tracks the consumer's location. Like other Google products, targeted advertisements appear across Google Maps.

G. Android and Google Play

65. Google's Android operating system was developed by Android, Inc., which Google acquired in 2005. Google partners with and licenses the use of Android to manufacturers of smartphones, tablets, digital assistants, and similar mobile devices, who pre-load such devices with the Android operating system. Android is the world's most widely used smartphone platform: as of late 2012, it enjoys 75% of worldwide smartphone market share (and over 50% of US market share), with 500 million devices activated. Google examines and certifies the compliance with Google's standards of each device that manufacturers seek to load with Android.

66. Google Play, formerly known as the Android Market, is the primary gateway for Android users to acquire, purchase, and download apps and other digital media for their Android devices. Google Play is operated by Google. Over 25 billion apps have been downloaded through Google Play.

67. Android device users must create an account to access Google Play. Once an account is created, all activity on the device, from web surfing and search query histories to app and media acquisition and usage, is recorded because users are permanently logged in. After Google's introduction of the new privacy policy on March 1, 2012, an Android device user's activity and personal information is aggregated with all of that user's other Google accounts in one comprehensive profile, so that such activity and personal information can be deployed in targeting ads to the user.

68. Android users can access Google+ and use the +1 feature in exactly the same way as any other Google user. Google treats +1 usage on Android devices in a manner that is, for all purposes relevant to this action, identical to its treatment of +1 usage on personal computers or non-Android devices.

69. Google causes certain personal information of every Android user that downloads an Android application through Google Play to be disclosed to the developer of the application downloaded. This disclosure occurs without the consent, authorization, or indeed the knowledge of the Android user. No notice is provided that the user's personal information is being or has been

disclosed to a third-party application developer, but several such developers have publicized this fact. The personal information so disclosed includes at least the name, email address, and physical or geographical location associated with the Play account and/or the Android device used to download the application.

70. The involuntary disclosure of such information to third-party application developers is an electronic transmission of data that consumes device battery power and bandwidth in measurable quantities. Both of these are commodities purchased by Android device users, not resources freely available in infinite supply.

H. Other Products

71. Google also offers dozens of other products and services. Google Docs (also known as Drive) allows consumers to create and edit documents online while collaborating in real-time with other consumers. Google Reader allows consumers to subscribe to, read, and share content. Google Blogger is Google's weblog publishing tool that allows consumers to share text, photos, and video. Picasa is Google's photo sharing tool that allows consumers to edit, post, and share digital photos. Targeted advertisements appear while consumers are using these products as well.

72. Google engages independent third-party entities to process user information and to distribute it across its various product platforms.

73. Each Google product logs and keeps track of different categories of information about the consumer. The following categories of personal information are collected by the various products:

- the consumer's first and last name;
- the consumer's home or other physical address (including street name and city or town);
- the consumer's current, physical location;
- the consumer's email address or other online contact information (such as a consumer's identifier or screen name);
- the consumer's IP address;

- the consumer's telephone number (including home and mobile telephone numbers);
- the consumer's list of contacts;
- the contents of consumers' Gmail messages (incoming and outgoing);
- the consumer's search history from Google's search engine and other query-based platforms, including YouTube;
- the consumer's web surfing history from cookies Google places on consumers' computers and other devices;
- the consumer's responsiveness to advertisements;
- all Android device activity, including app and media acquisition and usage; and
- all of the consumer's Google+ posts and "+1" usage across the internet.

Google vs. Facebook

74. Although Google ranks first in search-related ad revenues, its display advertising revenue is second to Facebook. Facebook garners a larger market share of display advertising revenue because consumers that use Facebook set up, manage, maintain, and populate personal profiles with very specific information about themselves. This allows Facebook to deploy a more complete picture of the individual to most effectively target advertisers' messages only to qualified consumers, providing advertisers the best return on their investments, using information each consumer willingly supplies to Facebook.

75. Unlike Facebook, a holistic view of each consumer was not available to Google until it changed its privacy policy on March 1, 2012. Prior to March 1, 2012, intended consumers were not easily identified by advertisers through Google. Google previously targeted its advertising using bits and pieces of anonymous information garnered from each discrete Google service. Because each Google product had a distinct privacy policy with non-identical terms, Google could not aggregate or combine data across its many platforms without violating the terms of its agreements with consumers.

76. James Whittaker, a former Google Engineering Director, described Facebook's advantage over Google when it came to profiting from user data. In a public explanation of his resignation, he wrote, on March 13, 2012:

> It turns out that there was one place where the Google innovation machine faltered and that one place mattered a lot: competing with Facebook…. Like the proverbial hare confident enough in its lead to risk a brief nap, Google awoke from its social dreaming to find its front runner status in ads threatened…. Google could still put ads in front of more people than Facebook, but Facebook knows so much more about those people.
>
> Advertisers and publishers cherish this kind of personal information, so much so that they are willing to put the Facebook brand before their own. Exhibit A: www.facebook.com/nike, a company with the power and clout of Nike putting their own brand after Facebook's? No company has ever done that for Google and Google took it personally.

77. Google's overhaul of its approach to privacy, which culminated in the implementation of the new unified privacy policy on March 1, 2012, is an attempt to squeeze more revenues out of its targeted ad system by, among other things, luring advertisers from Facebook to Google. Facebook set a new standard in targeted advertising because it had access to a relatively comprehensive profile of each user. Google could only compete by creating similar profiles of its users.

78. Indeed, although final full-year 2012 display ad revenues for Google and Facebook are not yet available, eMarketer, a widely trusted advertising market research firm, stated in September 2012 that Google was poised to surpass Facebook in display ad revenues for the first time. The fact that this gain correlates with Google's introduction of a unified privacy policy is not coincidental: Google attracts more advertisers because it has given itself access to a wealth of personalized data that was previously not available to it for cross-platform use. It can therefore target ads much more effectively.

79. However, Facebook users provide the information that goes into their profile willingly and voluntarily. Because Google agreed with its users before March 1, 2012 that it would only use the information they provided to Google for the purpose for which it was intended, namely to provide them with the service, Google could not simply construct individual user profiles; it had

1 to *cancel* the privacy policies in place when users agreed to create Google accounts and replace them
2 with a policy that permitted Google to create such a dossier. Additionally, the policy had to permit
3 Google to retroactively take advantage of users' activity prior to March 1, 2012 in constructing that
4 dossier.

5 80. As part of this privacy overhaul, Google also imitated Facebook's iconic personal
6 recommendation feature, called the "Like" button. When a user "Likes" a website, a brand, a
7 product, or other content on Facebook, that user's friends see the recommendation in their own news
8 streams, consisting typically of a thumbnail image depicting the thing recommended, a note that
9 "John Doe likes this," and a link to the website recommended. Facebook (and advertisers)
10 considered this personal recommendation feature a "holy grail of advertising" because users take
11 personal suggestions from friends much more seriously than anonymous corporate communications.
12 Google's imitation is the "+1" button. Google introduced the "+1" button on March 30, 2011, but
13 could not fully develop the concept until the privacy hurdles embedded in the multiplicity of policies
14 were cleared.

15 81. Google's personal recommendation system allows users to endorse products and
16 brands to their friends and contacts: Google says, "Click the +1 button to give something your public
17 stamp of approval." Google adds, "The next time your friends and contacts search on Google, they
18 could see your +1."

19 **<u>Google's Privacy Policies Before March 1, 2012</u>**

20 82. Prior to March 1, 2012, Google maintained more than 60 separate privacy policies for
21 its separate products.

22 83. Google formerly indicated, in a general overview of its approach to privacy, "When
23 you sign up for a particular service that requires registration, we ask you to provide personal
24 information. **If we use this information in a manner different than the purpose for which it was**
25 **collected, then we will ask for your consent prior to such use**."

26 84. Additional statements in specific privacy policies further indicated that Google would
27 use the consumer's personal information strictly in order to provide that particular product or service
28

to the consumer, and that Google would not use it for any other purpose without the consumer's consent. Indeed, in a legal notice issued to Gmail users in 2011, Google stated, "**We will not use any of your content [defined to include "text, data, information, images, photographs, music, sound, video, or other material"] for any purpose except to provide you with the Service**."

85. In addition, Google's prior Gmail privacy policy indicated, "Gmail stores, processes, and maintains your messages, contact lists, and other data related to your account **in order to provide the service to you**." Accordingly, Google's previous privacy policies indicated that Google would not use the consumer's personal information for any purpose other than that for which it was intended – to set up a specific account for a specific Google product.

86. Google has always maintained – and continues to maintain – that it will not sell or share with third parties a consumer's personally identifying information without the consumer's consent.

87. When Google implemented its unified privacy policy, Google violated these representations. All consumers, including each Plaintiff, that had a Google account and signed up to use Google products prior to March 1, 2012, when Google's new privacy policy took effect, agreed to create and use their various Google product accounts based on these representations. Their violation by Google has resulted in the invasion of the privacy interests of all Google users, including those of each Plaintiff, as explained in more detail below.

Google's New Privacy Policy

88. On March 1, 2012, Google announced that changes to its privacy policies had been made and that it had consolidated more than 60 of its privacy policies down to just one document.

89. As stated by Google, "Our new Privacy Policy makes clear that, if you're signed in, we may combine information you've provided from one service with information from other services."

90. Starting on March 1, 2012, Google began creating elaborate individual dossiers or profiles of its users. Whereas, prior to that date, a user's history of interactions with Google's various products was not available to any other product, as of that date, that history of interactions

became available – despite the express terms governing the users' engagement with each individual Google product, which prohibited such cross-pollination.

91. Thus, contrary to representations made in Google's prior privacy policies, Google's new privacy policy does not allow consumers to keep information about a consumer of one Google service separate from information gathered from other Google services.

92. Consumers are thus no longer able to restrain Google's use of the personal information they provided to Gmail, for example, to that service alone. Instead, Google combines information drawn from the consumer's Gmail account with information drawn from other Google services, such as Google+, Google's social network service.

93. In addition, Google now associates users' search histories with their Gmail and Google+ accounts and, therefore, builds detailed and accurate targeting segments for advertising purposes. Thus, Google now uses the consumer's actual gender and age to target that consumer for advertising, rather than its prior use of an anonymous profile created by algorithms that use web browsing history to target a consumer based upon a guess that the consumer is, for example, a female aged 30-45.

94. An example: instead of selling automobile advertisements to consumers Google marks as an "auto intender" merely based upon web-surfing and search history (which may include a 12 year old boy that can't drive or purchase a vehicle), Google can now scan a consumer's emails and Google+ account, confirm that the consumer is of driving age, and see that the consumer sent an email or blogged about shopping for a Mercedes-Benz. Thus, Google could now scan the Google+ or other accounts of the consumer's Gmail contacts and display a Mercedes-Benz advertisement to the consumer reflecting the endorsement of the consumer's Gmail contact. Google could also allow BMW to advertise its vehicles to that consumer, specifically trumpeting reviews that say BMW is better than Mercedes-Benz (for which BMW, in this example, would pay a premium). Thus, Google provides its advertisers with data that is specific, verified, and reliable, and advertisements can be personalized to each consumer's specific preferences, including implied endorsements from their

friends on Google+, Gmail contacts, and other individual users – all without the consent of the users and without compensating the users.

95. Further, when the consumer is not signed in to a Google account, Google continues to aggregate data in an anonymous profile. Google stores up to 180 days of signed-out search activity, including queries and results clicked in a cookie implanted on a consumer's computer or device. Now, when a consumer logs back into his or her Google account, that anonymous profile information is automatically appended to that consumer's account, at which point that anonymous information could be used to customize results for that consumer on that computer, or any other computer where the consumer is logged into a Google account.

96. Consumers of devices powered by Google's Android platform are automatically, and permanently, "logged in" for purposes of aggregation of their personal information. They have no way to opt out, and cannot avoid this unauthorized invasion of privacy unless they replace their Google Android device with a non-Android device, which costs hundreds of dollars.

97. All of this is designed to fuel advertising revenue. By providing search results that are tailored to the consumer, Google can keep consumers engaged and, therefore, using its products and services for longer periods of time. If consumers are using its products longer, Google can sell more advertising space because the advertising displays have more time to rotate.

98. As long as the consumer is signed in to any Google account, such as Gmail or Google+, Google will now aggregate in one profile all of the consumer's activity on any other Google product he or she utilizes. It will merge data from each of its platforms and services (including Android mobile devices), aggregating the content of the emails the consumer drafts, the content of emails the consumer receives, the searches the consumer conducts on google.com, the locations the consumer searches using Google Maps, the articles the consumer reads and pictures the consumer uploads to Google+; it is all combined to create a detailed profile of the consumer.

99. Google can also use this information to tailor the advertising to its intended user. If the consumer is located in Manhattan, Google can display advertisements only for restaurants located in Manhattan. More troublingly, if the consumer is considering purchasing a Mercedes-

Benz, Google can display advertisements endorsing Mercedes-Benz vehicles or competitor vehicles, depending on which company is willing to pay more for that ad.

100. Google also deploys targeted personal recommendations based on a user's contacts' use of the "+1" button. These endorsements are the most valuable aspect of the privacy overhaul because they allow advertisers to attach their brands to specific individuals with whom a user has an existing relationship (as evidenced by his or her communications with those individuals in Gmail, for instance).

101. Thus, by commingling data across Google products and optimizing search results, Google can: (1) keep consumers engaged longer, and longer engagement allows Google to sell and deliver more advertisements (engagement creates inventory); (2) display advertising that is specifically targeted to intended users, rather than the masses (which raises the likelihood that the consumer will click on the advertisement); and (3) display personal recommendations and endorsements for particular brands or products that appear to emanate from friends and contacts (which allows advertisers to overcome any resistance on the consumer's part relating to the trustworthiness of their marketing message). Google can, therefore, sell more advertisements *and* command a higher price for them, by delivering more intended users to its advertisers. The consumer's name and other personal information are associated with the Gmail or Google+ account (because the consumer provides that information to Google when he or she originally creates those accounts) and the consumer's identity is now associated with the whole spectrum of the consumer's internet activity. Google can now use that spectrum of data to sell advertisers the ability to target specific, intended consumers, rather than the masses.

102. Google's current ability to create a clear, well-rounded picture of the consumer – as opposed to its previous privacy policy that created largely anonymous puzzle pieces that could not be linked together (and were not always accurate) – is unquestionably invasive, and is being done in violation of its previous privacy policies pursuant to which the members of the Class agreed to utilize Google's products, and without the consumer's consent. Indeed, the new unified privacy

policy is emblematic of what former Google executive James Whittaker has called Google's recent shift from an "innovation factory" to "advertising company."

103. Not only has Google done so without each consumer's consent; it has not provided consumers with an effective way to opt out. While Google has made it very easy to universally merge data across product lines, it has not made it easy to opt out – consumers must manage their privacy settings for each Google product they use; a universal opt-out function is not available.

104. The thirty-six Attorneys General who on February 22, 2012 sent a letter to Google, opposing implementation of its new privacy policy, exposed Google's disingenuousness:

> Your company claims that users of Google products will want their personal information shared in this way because doing so will enable your company to provide them with a "simple product experience that does what you need, when you want it to," among many other asserted benefits. **If that were truly the case, consumers would not only decline to opt out of the new privacy policy, but would freely opt *in* if given the opportunity.** Indeed, an "opt-in" option would better serve current users of Google products by enabling them to avoid subjecting themselves to the dramatically different privacy policy without their affirmative consent. Unfortunately, Google has not only failed to provide an "opt-in" option, but has failed to provide meaningful "opt-out" options as well.

available at http://epic.org/privacy/google/20120222-Google-Privacy-Policy-Final.pdf.

105. Thus, Google's increased optimization comes at a significant cost to privacy and consumers' rights. What a consumer may discuss with friends on Gmail may be different than that which he or she would search on a computer at work. By commingling data (including searches, locations, and email contacts), and tying it to a specific Gmail account or Google+ account (and therefore a specific consumer), the consumer's personal information is no longer tied to the account; it is tied to an overarching profile in that person's name, that is regularly supplemented through use of or interaction with Google products. That person no longer remains anonymous where he or she intended to remain anonymous. The various portions of each person's life are no longer separate and treated in accordance with the expectation of privacy associated with each of them; they are no longer pieces to an impossible puzzle; they are pieces that can be, and as of March 1, 2012 have been, linked to create a clear picture of that consumer. The fact that this is achieved through independent third-party entities, the identities of which remain undisclosed, is immensely troubling.

Google's "+1" Feature

106. Because personal recommendations from friends and contacts enjoy substantially more persuasive power than an anonymous communication from a marketing department, Google, at the behest of the advertisers that drive its revenue, introduced the "+1" button on March 30, 2011. Under growing pressure from advertisers to penetrate more deeply into consumers' personal lives after Facebook's "Like" button revolutionized the way advertisers connect with individual consumers, Google made "+1" into a centerpiece of the Google+ product.

107. When it was initially rolled out, the +1 feature pertained only to search results on google.com. When it introduced the function, Google stated that the +1 button "enabl[es] you to share recommendations with the world right in Google's search results." Google touted +1 as "the digital shorthand for 'this is pretty cool.'"

108. Google also stated on March 30, 2011,

> To recommend something, all you have to do is click +1 on a webpage or ad you find useful. These +1's will then start appearing in Google's search results. Say, for example, you're planning a winter trip to Tahoe, Calif. When you do a search, you may now see a +1 from your slalom-skiing aunt next to the result for a lodge in the area. Or if you're looking for a new pasta recipe, we'll show you +1's from your culinary genius college roommate. And even if none of your friends are baristas or caffeine addicts, we may still show you how many people across the web have +1'd your local coffee shop.

109. Google introduced Google+ on June 28, 2011 and organized it around the +1 feature. All of a Google+ user's +1's appear in that user's "Posts" on Google+ and are accessible publicly. Though Google+ now includes a number of new features, the +1 function remains a core component of the Google+ product.

110. In October 2011, Google began incorporating +1 endorsements into graphical or display advertisements. In these visual ads, Google actually reproduces the pictures that users have submitted as their profile image or avatar just below the ad graphic, *directly associating user's faces with products or brands*.

111. Google+ offers its users no way to control who sees their +1's and regularly includes their +1's in advertisements and on third-party websites. As the quotation from Google reproduced

1 above suggests, Google displays +1's to other users based on their connections, including not only
2 their Google+ friends but, following the introduction of the new privacy policy on March 1, 2012,
3 also their Gmail contacts. A friend or contact of a Google+ user that clicked +1 for a particular
4 brand or product will be shown advertisements that indicate that that user +1'd the brand or product.
5 112. Google does not compensate the endorsers (those who click +1) for the use of their
6 likenesses in these personalized advertisements.
7 113. On its official blog for advertisers, Inside Adwords, Google described the +1 button
8 in the following way:
9
10
11
12
13
14
15

> Since its introduction on search results and search ads, the +1 button has been installed on over a million websites across the web with over 4 billion impressions daily. Starting early October [2011] we're expanding that to include display ads across the web on both desktop and mobile. For the first time, you'll be able to run social-enabled ad campaigns that work across millions of sites in over 40 countries around the world. If you're running display ads through the Google Display Network [a premium advertising network] you may begin seeing the +1 button and personal annotations with your ads. With a single click, people can recommend the ad's landing page to their friends and contacts. Incorporating personal recommendations into display ads has the potential to change the way people view advertising. ***A display ad becomes much more powerful when people can see which of their friends and contacts have chosen to endorse it***.

16 114. Google illustrated this concept as follows: "For example, take Elaine, who sees an ad
17 for discount flights. She +1's the ad, thinking her friends might value similar deals. Now when
18 Elaine's friends and contacts are logged into Google and see the discount flight ad on any of the
19 millions of [Google Display Network] partner websites, ***they'll see Elaine's picture across the***
20 ***bottom of the ad with a note saying she +1'd it***." This image accompanies that statement:
21
22
23
24
25
26
27
28

115. Google explains how it ensures that these endorsed ads are seen by the right contacts: "Elaine's friends and contacts will also be more likely to see the ad. Because a recommendation from a friend is such a strong signal of relevance, the Google Display Network gives ads that have been recommended an extra boost by including them in the auction for any page a friend visits."

116. Google offers its advertisers the ability to opt out of the +1 marketing scheme. However, it does not offer consumers the same courtesy.

117. Android users are able to use the +1 feature in exactly the same way as any other users, and Google processes +1's of Android users in the manner described above.

<u>Google's Concealed Disclosure of Android Users' Personal Information</u>

118. Google's Android mobile platform and Google Play marketplace are governed by the same unified privacy policy as its other product platforms, though they also have supplemental privacy terms.

119. Prior to March 1, 2012, the Android mobile platform and Google Play marketplace were governed by independent privacy policies.

120. In February 2013, American and international news media reported that Google has been, for an indefinite period, disclosing certain personal information of Android users to third parties that developed applications for Android. In particular, it was reported that each time an Android user accessed Google Play and downloaded and/or purchased an application, that user's

name, email address, and physical or geographical location was automatically transmitted from the user's Android device to the third-party application developer.

121. Android users are not notified of this automatic transmission involving their devices and their personal information, nor is their consent or authorization for this transmission sought.

122. Disclosure of this information is manifestly unnecessary to completing or processing any transaction. As Ben Edelman, a Harvard business professor, has explained, "it simply is not 'necessary' to provide developers with access to customer names or email addresses in order to process customer transactions. Apple has long run a similar but larger app marketplace without doing so."

123. This practice is contrary to the terms of both the old privacy policies and the new unified privacy policy – all of which state that user consent is required before Google can use personal information in ways other than that for which the information has been collected, and before Google can disclose users' personal information to third parties.

124. Google's surreptitious practice of causing such automatic transmissions came to light only thanks to the fact that one third-party application developer took to his blog to decry the practice.

125. Following initial reports, no other third-party application developers have contested the assertion that Google does, in fact, permit disclosure to them of the name, email address, and physical or geographical location of every Android user that downloads and/or purchases the applications they have placed in the Google Play marketplace, and certain self-interested entities, like the Application Developers Alliance, have announced their support of Google's practice.

126. This unauthorized disclosure subjects every affected Android app user to a substantially increased, unexpected, and unreasonable risk of further interception or dissemination of their personal information as well as of other adverse consequences, including harassment, receipt of unwelcome communications, and identity theft. The fact that third-party app developers have Android user data stored in their files makes such developers likely targets for hackers or others intent on acquiring that data, thanks to Google's practice. Where users leave bad feedback or critical

reviews of apps they've downloaded, the developers of such apps are able to respond directly to such users, thanks to Google's practice. Further, many Android app developers are non-professionals or coding hobbyists that simply paid a $25 entry fee to register and sell their creations in Google Play, and are unlikely to have sophisticated security measures in place, and are also likely to listen when cyber-criminals tell them they can make thousands by giving up their Play records. Every affected Android user is now subject to a heightened risk of these and other security events.

127. The secret transmission of personal information to third-party app developers begins from the Android user's device, and thus causes the depletion and consumption of device battery life and bandwidth, resources not freely available but purchased in finite quantities by Android users for their own exclusive use, not Google's.

<u>Plaintiffs' Injuries Resulting from Google's Privacy Overhaul</u>

128. Plaintiffs Marti, Nisenbaum, DeMars, Barrios, Anderson, Villani, and McCullough have suffered (and continue to suffer) pecuniary and non-pecuniary harms as a result of Google's conduct as alleged herein.

129. *First*, Plaintiff Marti has suffered, and continues to suffer, harm in the form of Google's unauthorized appropriation of his name and/or likeness in connection with its "+1" ad function. Google has incorporated Plaintiff Marti's recommendation or endorsement into visual display ads that have been shown to persons known to Google, thanks to its privacy overhaul, to be friends or contacts of Plaintiff Marti. When Google incorporates Plaintiff Marti's recommendation or endorsement into a visual ad that is shown to such users, or to millions of users not known to be Plaintiff Marti's friends or contacts, Google is injuring Plaintiff Marti.

130. *Second,* Plaintiff Nisenbaum has suffered harm in the form of the cost he paid to replace his Android-powered device after March 1, 2012. Plaintiff Nisenbaum acquired his Android device prior to the introduction of the new privacy policy and purchased an alternative, non-Android device (an Apple iPhone) after the introduction of the new privacy policy. As Google required him to do, he created an account to access Google Play prior to the introduction of the new privacy policy. His reason for switching to another mobile device is substantially that Google's new privacy

policy invades his privacy more than alternative mobile operating systems do, since it requires him to be permanently logged in to his account and aggregates, without his consent, all of his activity and other personal information associated with his Android device with all the other information Google has acquired from him in connection with other Google products, including Gmail. Had Google disclosed its intention to commingle all of Plaintiff Nisenbaum's Android-related personal information (including app acquisition and usage) with all other information available to Google via his use of other products, Plaintiff Nisenbaum would not have purchased an Android-powered device in the first place.

131. *Third*, Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough have suffered, and continue to suffer, harm in the form of the costs they have paid to provide their Android devices with the battery power and bandwidth necessary to disclose to third-party application developers the personal information that Google causes them to involuntarily disclose whenever they download an Android application. Each of these Plaintiffs, like every other Android device user that has downloaded at least one Android application through Google Play, has been compelled to transmit to the developers of the application or applications downloaded certain personal information, including the name, email address, and physical or geographical location associated with the Play account and/or the Android device used to download the applications. In every such transmission, device battery power was consumed without the Plaintiffs' consent, authorization, or knowledge. In every such transmission, bandwidth was also consumed without the Plaintiffs' consent, authorization, or knowledge. Each of these Plaintiffs has paid for the electricity required to charge his or her device and for the bandwidth required to download an application. Therefore, each of these Plaintiffs has suffered a measurable pecuniary injury.

132. *Fourth,* each Plaintiff suffered, and continues to suffer, an invasion of their privacy interests when the personal information that each provided in connection with discrete Google products prior to March 1, 2012 – including without limitation name, location, email address, email contacts, email message contents, query histories on various platforms, web browsing histories, and

declared preferences – was and is commingled with personal information provided in connection with other Google products prior to March 1, 2012 without any Plaintiffs' consent.

133. *Fifth*, each Plaintiff suffered, and continues to suffer, harm in the form of Google's unauthorized access and wrongful disclosure of each Plaintiff's communications. As alleged above, Plaintiffs – like all Gmail users – consented prior to March 1, 2012 to provide the Gmail service with information, including email communications drafted and received by each Plaintiff, *only* in connection with delivery of the service, and not for generalized, cross-platform use of that information by other Google products. Google's use of the contents of Plaintiffs' communications to inform their use of google.com, YouTube, Picasa, Google+, and other products is flatly inconsistent with the limited authorizations Plaintiffs granted to Google in connection with delivery of the Gmail service. By intentionally disclosing the contents of those communications outside of Gmail, Google has injured each Plaintiff. Further, insofar as Google engages independent, unidentified third-party entities to process and distribute user information across its product platforms, including the contents of Plaintiffs' Gmail communications, Google intentionally discloses the contents of those communications outside of Google, thus further injuring each Plaintiff.

134. *Sixth*, each Plaintiff suffered, and continues to suffer, harm in the form of Google's unauthorized interception of each Plaintiff's communications. When Google discloses the contents of Plaintiffs' Gmail communications to services other than Gmail, such as Google+ or google.com, the recipient service unlawfully acquires the contents of those communications and thus invades the legally protected rights of each Plaintiff. When Google goes further and discloses the contents of Plaintiffs' Gmail communications to independent, unidentified third-party entities to process and distribute user information across its product platforms, using an automatic routing mechanism that operates contemporaneously with the transmission of such communications, Google similarly invades the legally protected rights of each Plaintiff.

135. Finally, Google's invasion and exploitation of the privacy and legal interests of its users, including each Plaintiff, benefits Google in a quantifiable manner. Several injuries described

above are separately quantifiable, including (a) Google's appropriation for use in display ads of the names, images, identities or likenesses of users that click the +1 button, (b) the cost of device replacement for members of the Android Device Switch Subclass, and (c) the cost of resources, including battery power and bandwidth, necessary to carry out Google's concealed disclosure of Android user information to third-party application developers. However, because the monetary value of invaded privacy interests is less clear, Plaintiffs Marti and Nisenbaum have installed an internet browser plug-in called "Privacy Fix" that monitors their interaction with Google products and provides a figure representing the estimated value of each to Google based on their internet search activity. Plaintiffs submit that their privacy interests are quantifiable in this way, as alleged below.

A. Appropriations of Likeness

136. Plaintiff Marti created a Google+ account in 2011.

137. Plaintiff Marti did not agree to allow Google to use his name, photograph, or likeness in an advertisement as an endorsement.

138. In 2011, Plaintiff Marti uploaded a photo of himself to Google in connection with his Google+ account. That photo clearly bears his likeness.

139. Plaintiff Marti has clicked "+1" on YouTube videos, google.com search results, and on many third-party sites, including without limitation NYTimes.com, HuffingtonPost.com, and Flipboard.com.

140. Plaintiff Marti has clicked "+1" on such media and sites on both personal computers and on his Android-powered device.

141. Plaintiff Marti has been told by friends and contacts that they saw his name and/or face near or within "+1" display ads placed or managed by Google.

142. Plaintiff Marti has seen similar Google-placed or Google-managed ads indicating that his friends and contacts had clicked "+1" on or in connection with particular brands, products, and websites.

143. Plaintiff Marti has not been compensated for Google's commercial use of his personal endorsement of products, brands, and websites with which Google associated him and did not authorize Google's use of that endorsement.

144. Plaintiff Marti believes that his friends and contacts, the endorsements of whom were shown to him in Google-placed or Google-managed ads, were not compensated for Google's commercial use of their personal endorsement of the products, brands, and websites with which Google associated them and did not authorize Google's use of their endorsements.

145. Plaintiff Marti had a financial interest in the use of his identity and/or likeness in advertisements, but was deprived of that interest by Google.

B. Cost to Replace Android Devices

146. Plaintiff Nisenbaum acquired an Android-powered device in 2010 and continued to own that device on March 1, 2012, when the new privacy policy took effect.

147. Plaintiff Nisenbaum created an account in connection with his use of his Android device, as required by Google to access the Android Market (now Google Play).

148. Thereafter, Plaintiff Nisenbaum was permanently logged in to his Android-related account.

149. In connection with his registration of an account for use on his Android device, Google represented that it would "ask for [Plaintiff Nisenbaum's] consent prior to" any use "different than the purpose for which [the information collected in connection with Plaintiff Nisenbaum's use of his Android device] was collected."

150. Plaintiff Nisenbaum intended and reasonably believed that the information he provided in connection with his Android device and Android Market/Google Play account would not be used for any purpose other than to allow Google to provide him with access to the Android Market/Google Play.

151. Plaintiff Nisenbaum intended and reasonably believed that the information he provided in connection with his other Google accounts, including Gmail, would not be used for any purpose other than to allow Google to provide him with those other services.

152. On or around March 1, 2012, Google began combining information provided by Plaintiff Nisenbaum in connection with his Android device and his usage of the Android Market/Google Play with information provided in connection with other Google products – not to provide any particular service, but to create a more comprehensive and thus more lucrative representation of Plaintiff Nisenbaum.

153. Google did not seek or acquire Plaintiff Nisenbaum's explicit consent in combining the different categories of information that he provided in connection with the different services.

154. As a result of Google's aggregation of his Android-related information with his non-Android related information, Plaintiff Nisenbaum felt that his privacy interests were invaded and purchased an alternative, non-Android mobile device in or about May 2012.

155. Plaintiff Nisenbaum would not have purchased an Android device in 2010 if Google had disclosed that it would begin aggregating the information it collected in connection with Plaintiff Nisenbaum's use of the device, including his use of the Android Market/Google Play, with information Plaintiff Nisenbaum provided in connection with other Google products, including Gmail.

C. Cost of Device Battery Power and Bandwidth

156. Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough each acquired Android-powered devices prior to March 1, 2012 and continue to use Android-powered devices at present.

157. Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough each downloaded at least one Android application through Google Play on their Android devices.

158. Plaintiff Marti downloaded at least the following Android applications through Google Play: Words With Friends; Shazam; Photoshop Express; Talk; YouTube; What's App; NBC; Pandora; Navigator; Google+; Flixster; and Flipboard.

159. Plaintiff DeMars downloaded at least the following Android applications through Google Play: Chase Bank; Cracked Life; Flixster; Facebook; Angry Birds; and Bacon Reader.

160. Plaintiff Anderson downloaded at least the following Android applications through Google Play: Facebook; Shazam; Pandora; Words Free; and Yahoo Mail.

161. Plaintiff Villani downloaded at least the following Android applications through Google Play: Fidelity; Skype; a chess game.

162. Plaintiff McCullough downloaded at least the following Android applications through Google Play: Angry Birds; Backpacker GPS Trails Pro; Blast Monkeys; Dive Log; Dragon Fly! Free; Epistle; Facebook; Flixster; Google Sky Map; Handcent SMS; handyCalc; iBird Pro; JuiceDefender Pro; MoboPlayer; Pandora; reddit is fun; REI; Ringdroid; AAA Roadside; SDCard Manager; Shazam; TED; Google Translate; TripAdvisor; Wells Fargo; Where's My Droid; and Wiki Encyclopedia.

163. Every time Plaintiff Marti, DeMars, Barrios, Anderson, Villani, and McCullough downloaded an Android application through Google Play, unbeknownst to them, Google caused certain personal information belonging to them to be transmitted from their Android devices to the developer, or developers, of the application or applications downloaded.

164. The personal information so transmitted includes at least the name, email address, and physical or geographical location associated with the Android device and/or the Play account used to download the application.

165. Each such transmission required the consumption of Plaintiff Marti's, DeMars', Barrios', Anderson's, Villani's, and McCullough's device battery power, though they never consented or authorized Google to cause those transmissions.

166. Each such transmission also required the consumption of Plaintiff Marti's, DeMars', Barrios', Anderson's, Villani's, and McCullough's bandwidth, though they never consented or authorized Google to cause those transmissions.

167. Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough paid for the resources necessary to charge their Android-powered devices and to access the internet, including Google Play, and to download applications.

1 168. Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough have therefore
2 been deprived of the money they paid to charge their devices and to access the internet and
3 download applications in proportion to the unauthorized consumption of those resources caused by
4 Google's conduct in requiring certain personal information to be disclosed to third-party application
5 developers, as alleged above.

6 **D. Invasion of Privacy Interests**

7 169. Plaintiffs Marti, Nisenbaum, DeMars, Barrios, Anderson, Villani, and McCullough,
8 each created Gmail accounts prior to March 1, 2012.

9 170. The terms under which each Plaintiff agreed to create their Gmail accounts provided
10 that Google would (a) "ask for [Plaintiffs'] consent prior to" any use "different than the purpose for
11 which [the information collected in connection with the Gmail account] was collected"; (b) "not use
12 any of [Plaintiffs'] content for any purpose except to provide [Plaintiffs] with the Service"; and (c)
13 "store[], process[], and maintain[] [Plaintiffs'] messages, contact lists, and other data related to
14 [Plaintiffs'] account[s] in order to provide the service to you."

15 171. Plaintiffs Marti, Nisenbaum, DeMars, Barrios, Anderson, Villani, and McCullough,
16 each used and/or created accounts with other Google products prior to March 1, 2012, including
17 google.com, YouTube, Picasa, Voice, Google+, Maps, Docs, and other products.

18 172. In connection with their use and/or registration with these other Google products,
19 Google represented with respect to each that Google would "ask for [Plaintiffs'] consent prior to"
20 any use "different than the purpose for which [the information collected in connection with
21 Plaintiffs' use and/or registration with the other products] was collected."

22 173. Each Plaintiff provided Google with certain information, including their names, email
23 addresses, physical contact information, email contacts, and contents of emails drafted and received,
24 in connection with their Gmail accounts, and provided Google with *different* information, including
25 their search queries, web browsing histories, images, telephone contacts, locations, and video
26 consumption history, in connection with their other Google accounts and/or product usage.
27
28

1 174. Each Plaintiff intended and reasonably believed that the information he or she
2 provided in connection with Gmail would not be used for any purpose other than to allow Google to
3 provide each Plaintiff with the Gmail service.

4 175. Each Plaintiff intended and reasonably believed that the information he or she
5 provided in connection with the other Google products would not be used for any purpose other than
6 to allow Google to provide each Plaintiff with those other services.

7 176. On or around March 1, 2012, Google began combining information provided by each
8 Plaintiff in connection with Gmail with information provided in connection with the other Google
9 products – not to provide any particular service, but to create a more comprehensive and thus more
10 lucrative representation of each individual Plaintiff.

11 177. Google did not seek or acquire the explicit consent of any Plaintiff in combining the
12 different categories of information that they provided in connection with the different services.

13 178. Moreover, each Android user that downloaded and/or purchased an app through
14 Google Play is subject to an increased, unexpected, and unreasonable risk of further invasions of
15 privacy, and of harassment, identity theft, and other security events, thanks to Google's practice of
16 disclosing to third-party app developers such users' personal information in every Play transaction.

17 **E. Unauthorized Access and Wrongful Disclosure of Communications**

18 179. Plaintiffs Marti, Nisenbaum, DeMars, Barrios, Anderson, Villani, and McCullough,
19 each consented prior to March 1, 2012 to provide information to the Gmail service *only* to allow
20 Google to provide them with the Gmail service. No Plaintiff agreed to grant Google a generalized
21 license to combine their Gmail information, including contact lists and specific email
22 communications, with information obtained through their use of products other than Gmail.

23 180. On or around March 1, 2012, Google accessed each Plaintiff's stored email
24 communications (in Gmail) and made their contents available to products other than Gmail,
25 including google.com search, Picasa, Voice, Google+, Maps, Docs, and other products.

26 181. Such access was not accidental but was done pursuant to the new unified privacy
27 policy introduced on March 1, 2012.

28

182. After March 1, 2012, each Plaintiff began to receive google.com search results and to be shown ads, on various Google products and on third-party websites participating in Google advertising networks, that draw information from their Gmail activity, including the contents of the messages in their Gmail boxes, and are tailored to specific interests described in their messages and locations described in their messages or derived from personal information provided to Gmail but not to google.com or any other Google product.

183. Further, insofar as Google engages independent, unidentified third-party entities to process and distribute user information across its product platforms, including the contents of Plaintiffs' Gmail communications, Google intentionally discloses the contents of those communications outside of Google.

F. Unauthorized Interception of Communications

184. Plaintiffs Marti, Nisenbaum, DeMars, Barrios, Anderson, Villani, and McCullough, each consented prior to March 1, 2012 to provide information to the Gmail service *only* to allow Google to provide them with the Gmail service. No Plaintiff agreed to grant access to such information to any service other than Gmail, or for any purpose other than to permit Google to provide them with the Gmail service.

185. On or around March 1, 2012, each Plaintiff's Gmail communications, including but not limited to communications sent by Plaintiffs and en route to their destinations in other users' e-mailboxes as well as communications sent to Plaintiffs and en route to their destinations in Plaintiffs' e-mailboxes, were accessed by Google products other than Gmail, including google.com search, Picasa, Voice, Google+, Maps, Docs, and others. Such access occurred through Google's use of computer systems, applications, and/or codes that were not necessary to deliver the Gmail service to Plaintiffs, but which were designed to export portions of the contents of each Plaintiff's Gmail communications to other services or products and for use on third-party sites that have partnered with Google in advertising networks. As described above, the Gmail platform has in place an automatic mechanism that routes incoming and outgoing messages contemporaneously to independent third parties – not, or not only, to facilitate the transmission of such messages, but to

distribute portions or derivations of the contents of Gmail communications to other Google services for use in those other services and in advertising on third-party websites that have partnered with Google in advertising networks.

186. Plaintiffs know this because, after March 1, 2012, each Plaintiff began to receive google.com search results and to be shown ads, on various Google products and on third-party websites participating in Google advertising networks, that draw information from their Gmail activity, including the contents of the messages in their Gmail boxes (including the Sent mailbox, which contains messages that are en route to their destination in other users' e-mailboxes), and are tailored to specific interests described in their messages and locations described in their messages or derived from personal information provided to Gmail but not to google.com or any other Google product.

G. Quantification of Invaded Privacy Interests

187. Plaintiffs Marti and Nisenbaum each installed an internet browser plug-in called "Privacy Fix" to compute the monetary value of their invaded privacy interests to Google.

188. Privacy Fix works by calculating how many Google-placed and Google-managed targeted advertisements a user is exposed to when conducting internet searches. It therefore does not take into account all aspects of a user's internet existence, but represents a baseline valuation of a user's information insofar as it is used by Google to target advertisements at the user.

189. Privacy Fix reports its quantification in a table called, "What are you worth?" In that table, the plug-in provides a monetary figure and states, "Google makes about this much per year from ads at your level of activity."

190. Privacy Fix reported that Plaintiff Marti was "worth" about $7.44 per year to Google based on his search activity (i.e., not taking into account the value of his misappropriated likeness, as alleged above).

191. Privacy Fix reported that Plaintiff Nisenbaum was "worth" about $2.23 per year to Google based on his search activity.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Ongoing Governmental Investigations Regarding Google's Violations of the Privacy and Legal Rights of Its Users Demonstrate the Seriousness of the Injuries that Google's New Privacy Policy Has Inflicted on the Class

192. Google's conduct as herein alleged, and the injuries caused to the Plaintiffs, are consistent with its historical practice of violating the privacy of the consumers of its products and its disrespect for legal rights.

A. FTC Penalty Concerning Google Buzz

193. In February 2010, Google launched a social networking service called Google Buzz, which is the antecedent of Google+. Two of Google Buzz's key features were called "Rich fast sharing" (which combined a variety of social media sources such as Picasa and Twitter into a single news feed), and "Automatic friends lists" (consumers' Gmail contacts were automatically added to a consumer's Google Buzz account). Thus, Google Buzz was Google's first attempt at cross-pollinating content across different Google products. Google took information consumers provided for use within one Google product, Gmail, and used it to populate Google Buzz, a separate Google product.

194. Google transferred this information despite the fact that, as described above, Google's prior privacy policies stated that Google would only use a consumer's Gmail information for the purpose of providing Gmail services, and would not use this information for any other purpose without the consumer's consent. Contrary to its terms of service, however, Google was using consumers' Gmail information to populate Google Buzz.

195. Such cross-referencing of data harmed all consumers by violating their expectation of privacy in their emails and contact lists; but Google's practice was particularly harmful to clients of mental health professionals, attorneys, and finance professionals, as well as to the professionals themselves, who must promise confidentiality.

196. Not only did Google cross-index this information between products without consumers' consent, but Google did not adequately disclose that Google was automatically making certain private information public through use of the Google Buzz product, and there was no clear way for a consumer to opt out of Google Buzz or to make the information non-public. Indeed,

options for controlling the privacy of this information were very difficult to locate and confusing to consumers.

197. These unfair and deceptive trade practices resulted in an October 13, 2011 Consent Order between Google and the Federal Trade Commission ("FTC"). The FTC found that Google "failed to disclose adequately that consumers' frequent email contacts would become public by default."

198. The FTC also found that controls for limiting disclosure of personal information were "confusing and difficult to find…."

199. Further, the "options for declining or leaving the social network were ineffective."

200. Google had also failed "to give consumers notice and choice before using their information for a purpose different from that for which it was collected."

201. In announcing the Consent Order, Jon Leibowitz, Chairman of the FTC, stated, "when companies make privacy pledges, they need to honor them."

202. The FTC found that Google deceptively claimed that it would seek consumers' consent before using their information for a purpose other than that for which it was collected; Google misrepresented the consumers' ability to exercise control over their information; and Google misrepresented the extent of its compliance with the U.S.-EU Safe Harbor Framework by claiming that the company complied with the framework while violating the principles of Notice and Consent.

203. In addition to these findings, the Consent Order governs Google's current and future conduct. Part I of the Consent Order prohibits Google from misrepresenting: (a) the extent to which it "maintains and protects the privacy and confidentiality" of personal information; and (b) the extent to which it complies with the U.S.-EU Safe Harbor Framework. Part II of the Consent Order requires Google to obtain "express affirmative consent" before "any new or additional sharing by [Google] of the Google user's identified information with any third party…."

204. On February 13, 2013, the public learned that Google is flouting this Consent Order by requiring the automatic disclosure to third-party Android application developers of Android

device users' names, email addresses, and physical or geographical locations, whenever such users download an application.

205. Prior to February 13, 2013, Android device users did not know that Google was disclosing their personal information to third-party application developers each time they downloaded an application. Indeed, because the transmission of such information occurs without notifying Android users, they could not have known this was the case until one of the third-party application developers came forward and informed the public. Since then, other application developers have confirmed that such personal information is transmitted to them each time the application they have created, or which they market, is downloaded.

206. The risks associated with such unconsented – and concealed – disclosure of personal information include an increased likelihood of suffering identity theft or having malware implanted on one's device, because the application developers in receipt of such information may decide to sell pools of personal data to malicious groups, or because those developers may themselves suffer security breaches.

207. Google has not admitted to this conduct.

B. FTC Penalty Concerning DoubleClick

208. Google continued to disregard its customers' concerns about and interests in their privacy by blithely violating its obligations under the FTC Consent Order. On August 8, 2012, the FTC filed a complaint in the U.S. District Court for the Northern District of California against Google, charging Google with having misrepresented to users of Apple, Inc.'s Safari internet browser that it would not place tracking cookies or serve targeted ads to those users and that users would automatically be opted out of such tracking and targeting as a result of the default settings of the Safari browser.

209. According to the FTC's complaint, Google specifically told Safari users that because the Safari browser is set by default to block third-party cookies, as long as users did not change their browser settings, this setting "effectively accomplishes the same thing as [opting out of this particular Google advertising tracking cookie]." In addition, Google represented that it is a member

of an industry group called the Network Advertising Initiative, which requires members to adhere to its self-regulatory code of conduct, including disclosure of their data collection and use practices.

210. Despite these promises, the FTC charged that Google placed advertising tracking cookies on consumers' computers, in many cases by actively circumventing the Safari browser's default settings. Google exploited an exception to the browser's default setting to place a temporary cookie from the DoubleClick domain. Because of the particular operation of the Safari browser, that initial temporary cookie opened the door to all cookies from the DoubleClick domain, including the Google advertising tracking cookie that Google had represented would be blocked from Safari browsers.

211. Google's actions expressly violated the FTC's October 2011 Consent Order which barred Google from, *inter alia*, misrepresenting the extent to which consumers can control the collection of behavioral and related information.

212. The FTC's action was settled pursuant to a new Consent Order, dated August 9, 2012, that required Google to pay a record $22.5 million and required Google to disable all tracking cookies it had said it would not place on consumers' computers.

213. In announcing the Order, FTC Chairman Jon Leibowitz said, "No matter how big or small, all companies must abide by FTC Orders against them and keep their privacy promises to consumers, or they will end up paying many times what it would have cost to comply in the first place."

C. The European Union's Investigation of Google's New Privacy Policy

214. As set forth above, on March 1, 2012, Google changed its privacy policy, which, yet again, allows the commingling of user data between Google's products without consumers' consent or an effective ability to opt out. It commingles data in the same manner that resulted in the October 2011 Consent Order, and consumers of Google's products and services have been harmed as a result.

215. The new privacy policy came under governmental scrutiny in Europe last year, and the investigation of European Union ("EU") authorities was still ongoing as of the date of filing of this Consolidated Amended Complaint.

216. On February 2, 2012, the EU notified Google CEO Larry Page ("Page") that an Article 29 Working Party – an "independent European advisory body on data protection and privacy" – would be reviewing "the possible consequences for the protection of the personal data of [EU member state] citizens in a coordinated procedure." The Article 29 Working Party designated a French national regulatory body, the National Commission for Computing and Civil Liberties ("CNIL"), to lead the investigation.

217. In the same letter, the Article 29 Working Party "call[ed] for a pause [on Google's behalf] in the interests of ensuring that there can be no misunderstanding about Google's commitments to information rights of their users and EU citizens, until we have completed our analysis."

218. On February 27, 2012, the CNIL informed Page of the CNIL's preliminary findings. According to the letter, "[the CNIL's] preliminary analysis shows that **Google's new policy does not meet the requirements of the European Directive on Data Protection** (95/46/CE), especially regarding the information provided to data subjects" (emphasis in original). To comply, the CNIL explained, Google would have to provide more specific disclosures about how it plans to use different categories of user information.

219. The CNIL further observed that, "rather than promoting transparency, the terms of the new policy and the fact that Google claims publicly that it will combine data across services raises fears about Google's actual practices. Our preliminary investigation shows that it is extremely difficult to know exactly which data is combined between which services for which purposes, even for trained privacy professionals."

220. The same letter adds, "**The CNIL and the EU data protection authorities are deeply concerned about the combination of personal data across services: they have strong doubts about the lawfulness and fairness of such processing, and about its compliance with European Data Protection legislation**…" (emphasis in original). The letter concludes by "**reiterat[ing], on behalf of the Working Party, our call for a pause until we have completed our analysis**" (emphasis in original).

221. The CNIL sent Page another letter on March 16, 2012, in which it stated, "The CNIL deeply regrets that Google did not delay the application of the new policy, despite the first conclusions of our analysis regarding its compliance with the European data protection legislation."

222. The March 16, 2012 letter annexed a questionnaire containing 69 questions regarding Google's new privacy policy. A second questionnaire was sent to Google on May 22, 2012 because Google's responses were inadequate, imprecise, or incomplete.

223. On October 16, 2012, the Article 29 Working Party sent Page a letter outlining the CNIL investigation findings. After noting that the new privacy policy "suggests the absence of any limit concerning the scope of the collection and the potential uses of the personal data" of users, the letter presents a series of legal deficiencies associated with the new privacy policy. Most importantly, the letter states that "**the investigation confirmed our concerns about the combination of data across services**" (emphasis in original).

224. Based on the CNIL's investigation, it is now clear that, "The new Privacy Policy allows Google to combine almost any data from any services for any purpose." Because Google has failed to obtain user consent, and has failed to limit or to balance its data collection and cross-platform sharing practices, the CNIL stated that, "Combining personal data on such a large scale creates high risks to the privacy of users. Therefore, Google should modify its practices when combining data across services for these purposes."

225. The CNIL investigation also confirmed that Google's new policy provides insufficient information to users about what kinds of data will be collected and shared with different services, and the purposes for which such data will be collected and shared with different services.

226. The CNIL offered Google several practical recommendations. Regarding combination of data, the CNIL stated that "Google should take action to clarify the purposes and means of the combination of data. In that perspective, Google should detail more clearly how data is combined across its services and develop new tools to give users more control over their personal data," and that Google should provide an opt-out mechanism that would allow users to prevent Google from aggregating their personal data.

227. In its formal findings, the CNIL made clear that "**Google's interests** to implement the extensive combination of data detailed above **are overridden by the interests for fundamental rights and freedoms of the data subject** [i.e., user]" (emphasis in original).

228. Google was given until February 2013 to respond adequately and completely to the CNIL's queries, and to explain how it plans to bring its new unified privacy policy into line with the EU's legal requirements. The deadline for a response was February 18, 2013, and Google failed to make any further reply or to implement a less restrictive, more transparent privacy policy.

229. On February 18, 2013, the CNIL stated that it would lead a new Working Group that would impose a penalty or other repressive measures against Google by summer 2013. The EU authorities have not yet announced the nature or severity of the repressive measures they expect to impose on Google.

230. Other regulatory organizations representing the interests of states and citizens outside of Europe, including the Asia Pacific Privacy Authorities (which comprises privacy authorities of Australia, Canada, Hong Kong, Korea, Mexico, and New Zealand), conducted investigations into Google's new privacy policy, and pleaded with Google to grant more control to users regarding the manner in which their personal data is handled and to clarify the extent to which personal data is shared across Google products.

Consumers Do Not Want Google to Aggregate Their Information

231. Studies show that an overwhelming number of consumers do not want to receive advertisements targeted based on behavior or the contents of their emails, or search results based on their prior activity and behavior on other platforms, such as Gmail.

232. According to a March 9, 2012 study released by the Pew Internet & American Life Project, 800 Web users were asked how they would feel about a search engine remembering their prior queries and using that data to personalize future results. Seventy-three percent of the respondents said they "would not be okay with it" because they felt it was an invasion of privacy.

233. The study also asked 1,700 Web users how they felt about receiving targeted advertisements. Sixty-eight percent of respondents were "not okay with it" because they do not want

to be tracked and profiled. Only 28% said they were "okay with it" because they received ads and information relevant to their interests.

234. These results are consistent with a study released in September of 2009 by professors at the University of Pennsylvania's Annenberg School for Communication and the University of California, Berkeley School of Law, which found that sixty-six percent of Web users do not want customized ads.

235. Seizing on the rampant unpopularity of Google's new privacy policy and its invasive advertising practices, Microsoft, which operates Outlook.com, launched a new campaign to promote its service over Gmail on the premise that Outlook.com respects user privacy more than Gmail. To bolster its promotion (labeled, "Don't Get Scroogled"), Microsoft commissioned research on consumer perceptions of Google's practices.

236. Microsoft hired GfK Roper to conduct field research on February 1-4, 2013 and issued its results on February 7, 2013. The research indicates that 47% of internet users did not believe that any major email service providers scan the contents of their personal emails to target ads to them, while 19% did not know; only 34% believed, accurately, that some email providers do scan the contents of their emails for advertising purposes.

237. The research also indicated that 89% of internet users disapprove of the notion that email providers would scan the contents of their personal emails to target ads to them.

238. The research also showed that 86% of internet users feel that email providers' scanning of their personal emails to target ads to them is an invasion of their privacy. 90% of internet users agreed that this practice should not be allowed. 87% also agreed that email providers should allow users to opt out of such content-scanning.

239. As alleged more fully elsewhere herein, Google not only scans the contents of Gmail users' emails in order to target ads to those users within Gmail; Google goes much further and *discloses the contents of those communications to entirely different services* (and unidentified third-party processing entities), in contravention of the pre-March 1, 2012 privacy policies, in

1 contravention of users' reasonable expectations of privacy, and in contravention of common law and
2 statutory protections afforded to Google's users.

3 **TOLLING OF THE STATUTE OF LIMITATIONS**

4 240. There is no way to categorically opt out of Google's new privacy policy. The
5 existing means of opting out are limited, partial, and not readily ascertainable. A user would have to
6 abstain from using Google products to effectively prevent Google from conducting the invasive and
7 injurious actions complained of herein. Accordingly, exercising reasonable care, Plaintiffs and the
8 Class and Subclass members cannot effectively opt out of Google's new privacy policy.

9 241. By reason of the foregoing, the claims of Plaintiffs and other Class and Subclass
10 members are timely under any applicable statute of limitations (as tolled by the filing of the initial
11 Complaint) pursuant to the discovery rule and the doctrine of fraudulent concealment.

12 242. Google has been aware of the deceptive nature of its prior privacy policies at least
13 since the decision was made to collapse most of the discrete privacy policies into one, near the end
14 of 2011 and likely much earlier.

15 243. Despite this knowledge and awareness, Google continues to aggregate consumers'
16 personal data without their consent and a meaningful ability to opt out.

17 244. Google's failure to obtain consumers' explicit consent to the practice of combining
18 and sharing or disclosing users' personal information across its platforms and in the compilation of a
19 comprehensive individual dossier for each user, its failure to provide a meaningful opt-out
20 mechanism, and its failure to compensate users the likenesses of whom are incorporated into
21 Google-managed ads was and is willful, wanton, malicious, outrageous, and was and continues to be
22 undertaken in deliberate disregard of, or with reckless indifference to, the rights and interests of
23 Plaintiffs and the Class and Subclass members.

24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

COUNT I

VIOLATION OF CALIFORNIA'S RIGHT OF PUBLICITY STATUTE

California Civil Code § 3344

(On Behalf Of The Class)

245. Plaintiffs reallege and incorporate by reference each and every allegation set forth above as though fully set forth herein.

246. California's Right of Publicity statute, Cal. Civ. Code § 3344, protects persons from the unauthorized misappropriation of the person's identity or likeness by another for commercial gain.

247. During the Class Period, Google knowingly used Plaintiff Marti's name, face, and/or likeness, and those of members of the Class, for advertising, selling, soliciting, or other commercial purposes. Users of Android-powered devices, including Plaintiff Marti, were affected in exactly the same respect as all other users of Google services.

248. Google did not obtain Plaintiff Marti's or other members of the Class' consent to do so.

249. Although Plaintiff Marti's and other Class members' names, images, and likenesses possess pecuniary value by virtue of enhancing the value of targeted advertising, Plaintiff Marti and other Class members received no compensation or other consideration for Google's use thereof.

250. Plaintiff Marti and members of the Class were therefore injured by Google's actions.

251. The advertisements that misappropriated Plaintiff Marti's and other Class members' names, images, and likenesses were not used in conjunction with news, public affairs, sports broadcasts or accounts, or political campaigns.

252. Each incident is a separate and distinct violation of California Civil Code § 3344.

253. Plaintiff Marti and members of the Class therefore seek injunctive relief, and other such preliminary and other equitable or declaratory relief as may be appropriate.

254. Plaintiff Marti and members of the Class also seek remedy as provided by California Civil Code § 3344(a) in an amount equal to the greater of $750 per incident, or the actual damages

suffered as a result of the unauthorized use, and any profits derived by Google from that unauthorized use and are not taken into account in computing the actual damages, as well as punitive damages, attorneys' fees and costs, and any other relief as may be appropriate.

COUNT II

COMMON LAW COMMERCIAL MISAPPROPRIATION

(On Behalf Of The Class)

255. Plaintiffs reallege and incorporate by reference each and every allegation set forth above as though fully set forth herein.

256. A common law claim for commercial misappropriation protects persons from the unauthorized appropriation of the person's identity by another for commercial gain.

257. During the Class period, Google knowingly used Plaintiff Marti's and other Class members' names, images, and/or likenesses for advertising, selling, soliciting, or other commercial purposes. Users of Android-powered devices were affected in exactly the same respect as all other users of Google services.

258. Google did not obtain Plaintiff Marti's or other Class members' consent to do so.

259. Plaintiff Marti and other Class members received no compensation or other consideration for Google's use thereof.

260. Plaintiff Marti and members of the Class were harmed by Google's actions.

261. Plaintiff Marti and members of the Class therefore seek injunctive relief, and other such preliminary and other equitable or declaratory relief as may be appropriate.

262. Plaintiff Marti and members of the Class also seek actual damages suffered as a result of the unauthorized use, disgorgement of all profits from the unauthorized use that are attributable to the unauthorized use, punitive damages, attorneys fees and costs, and any other relief as may be appropriate.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

COUNT III

VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code § 17200, *et seq.*

(On Behalf Of The Class)

263. Plaintiffs reallege and incorporate by reference each and every allegation set forth above as though fully set forth herein.

264. As described above (Counts I and II), Google's nonconsensual use of Plaintiffs' and the Class' personal information, including Google's nonconsensual commercial use of Plaintiff Marti's name, image, and/or likeness in advertisements, violates the California Right of Publicity statute and common law principles of commercial misappropriation.

265. As described below (Count VI), Google's nonconsensual use of Plaintiffs' and the Android Device Switch Subclass' personal information, including Google's nonconsensual use of Plaintiff Nisenbaum's Android-related information and activity in connection with his non-Android-related personal information and activity on other products, violates California's Consumer Legal Remedies Act.

266. As described below (Counts IX and X), Google's nonconsensual use of Plaintiffs' and the Class' personal information, including the unauthorized access, interception, and disclosure of the contents of Plaintiffs' electronic communications and other data, violates the Federal Wiretap Act and the Stored Electronic Communications Act.

267. These violations therefore satisfy the "unlawful" prong of the Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq.*

268. Google also violates the "fraudulent" prong of the UCL by intentionally and knowingly misrepresenting that Plaintiffs and the Class have full control to prevent their appearance in advertising on Google's products. Google does so with the intent of inducing members to register for, and to use, its products and services, and to participate in advertisements even while Google knows there is no meaningful way to prevent one's name, photograph, likeness, or identity from being used in advertising or appearing as an endorsement in advertisements.

269. Moreover, Google intentionally misrepresented Plaintiffs' and the Class' ability to prevent use of his or her appearance and personal information in advertisements so Google could enjoy substantial profits by having users unwittingly appear in such advertisements.

270. Plaintiffs and the Class justifiably relied upon those misrepresentations when deciding to sign up for and use Google's products and services, and when using those services to run searches for their interests, exchange emails with contacts, edit and share their pictures, stream videos, and search for directions, among other things. Plaintiffs and the Class suffered damages of deprivation of money earned by the misrepresentations, in an amount to be proven at trial.

271. Google violated the "unfair" prong of the UCL by leading Plaintiffs and the Class to believe that they could opt out of advertising endorsements, encouraging Plaintiffs and the Class to make Google products indispensable to their lives, and then using Plaintiffs' and the Class' personal information in a manner in which Plaintiffs and the Class cannot effectively opt out.

272. Google violated the "unfair" prong of the UCL further by intentionally profiting from the nonconsensual, unauthorized endorsements extracted from Plaintiff Marti and other Class members without sharing those profits with Plaintiff Marti and the Class.

273. Google's unfair, deceptive, and fraudulent practices originated from California. In addition, decisions concerning Google's privacy policies and advertising decisions were made in California.

274. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and the Class seek an order from this Court permanently enjoining Google from continuing to engage in the unlawful, unfair, and fraudulent conduct described herein. Plaintiffs and the Class seek an order requiring Google to (1) immediately cease the unlawful practices described in this Complaint; and (2) award Plaintiffs and the Class reasonable costs and attorneys' fees pursuant to Cal. Code of Civ. Proc. § 1021.5.

275. Plaintiffs and the Class have vested, monetary interests in the use of their personal information to target advertising and in their appearance or representation in Google advertisements, and Google has deprived them of these interests. Moreover, Plaintiffs Marti and Nisenbaum have quantified the value to Google of their privacy interests invaded in connection with their internet

search activity, as alleged above. Plaintiffs are entitled to restitution of the sums by which they have been made to unjustly enrich Google.

276. Furthermore, Plaintiff Marti and the members of the Class have each lost money to which they were entitled in the form of compensation for the use of their images, names, and likenesses, in which they had a vested interest, by virtue of Google's conduct. They are entitled to restitution of such sums.

COUNT IV

BREACH OF CONTRACT

(On Behalf Of The Class)

277. Plaintiffs reallege and incorporate by reference each and every allegation set forth above as though fully set forth herein.

278. Prior to March 1, 2012, Google's privacy policies stated, "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." However, "the purpose for which [user data] was collected" was to create and manage users' accounts. It was not provided for tracking or advertising, and certainly not for advertising *outside of* the services within which the information was originally provided, and no users of Google services agreed to have Google consolidate their data across over sixty independent services for advertising purposes. Plaintiffs and the Class did not consent to the change in the privacy policies introduced on March 1, 2012 because there is no simple, effective way to provide consent or to opt out.

279. Between July 1, 2004 and March 11, 2009, Google's privacy policies stated that, while there may be changes to those policies, "we expect most such changes to be minor." Eliminating the individual privacy policies of nearly every Google service is not minor. Consolidating user data across nearly every Google service is not minor.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

280. Google breached its contract with Plaintiffs and the Class by consolidating and sharing user data across dozens of its services for advertising purposes without first obtaining user consent.

281. Google further breached its contract with Plaintiffs and the Class by failing to provide a simple and effective means of opting out of the consolidated privacy policy and Google's practice of consolidating user data across dozens of services.

282. Google also breached its contract with Plaintiffs and the Class by enacting a major change in its privacy policies when it eliminated them entirely in favor of a single, unified policy with terms substantially different than those in effect when Plaintiffs and the Class initially acquired Google accounts, prior to March 1, 2012.

283. Plaintiffs and the Class have suffered and will continue to suffer damages including, without limitation, deprivation of money earned by the misuse of their personal information by Google, invasions of their privacy interests (which, insofar as those interests pertain to internet search activity, have been quantified by Plaintiffs Marti and Nisenbaum), and loss of personal information, all of which have ascertainable value to be proven at trial.

COUNT V

COMMON LAW INTRUSION UPON SECLUSION

(On Behalf Of The Class)

284. Plaintiffs reallege and incorporate by reference each and every allegation set forth above as though fully set forth herein.

285. Google invaded upon something secret, secluded or private pertaining to the Plaintiffs and the Class, including without limitation contents of Gmail communications and Gmail contact lists, web search and web surfing histories, and other information in which Plaintiffs and the Class have a reasonable expectation of privacy.

286. Google's actions constitute an impermissible intrusion upon Plaintiffs' and the Class' seclusion or solitude, and/or their private affairs.

287. Google's invasion would be highly offensive to a reasonable person, as evidenced for instance by the allegations contained in the section titled, "Consumers Do Not Want Google to Aggregate Their Information."

288. Google's invasion violates expectations of privacy that have been established by general social norms.

289. Moreover, Plaintiffs Marti and Nisenbaum have quantified the value to Google of their privacy interests invaded in connection with their internet search activity, as alleged above.

290. Plaintiffs and the Class were damaged by such unauthorized actions in amounts to be proven at trial.

COUNT VI

VIOLATIONS OF CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT

California Civil Code § 1750 *et seq.*

(On Behalf Of The Android Device Switch Subclass)

291. Plaintiffs reallege and incorporate by reference each and every allegation set forth above as though fully set forth herein.

292. As described above, Plaintiff Nisenbaum acquired an Android-powered device in 2010 and continued to own that device on March 1, 2012, when the new privacy policy took effect. Plaintiff Nisenbaum created an account in connection with his use of his Android device, as required by Google to access the Android Market (now Google Play).

293. Thereafter, Plaintiff Nisenbaum was permanently logged in to his Android-related account. In connection with his registration of an account for use on his Android device, Google represented that it would "ask for [Plaintiff Nisenbaum's] consent prior to" any use "different than the purpose for which [the information collected in connection with Plaintiff Nisenbaum's use of his Android device] was collected."

294. Plaintiff Nisenbaum intended and reasonably believed that the information he provided in connection with his Android device and Android Market/Google Play account would not

1 be used for any purpose other than to allow Google to provide him with access to the Android
2 Market/Google Play.

3 295. Plaintiff Nisenbaum intended and reasonably believed that the information he
4 provided in connection with his other Google accounts, including Gmail, would not be used for any
5 purpose other than to allow Google to provide him with those other services.

6 296. On or around March 1, 2012, Google began combining information provided by
7 Plaintiff Nisenbaum in connection with his Android device and his usage of the Android
8 Market/Google Play with information provided in connection with other Google products – not to
9 provide any particular service, but to create a more comprehensive and thus more lucrative
10 representation of Plaintiff Nisenbaum.

11 297. Google did not seek or acquire Plaintiff Nisenbaum's explicit consent in combining
12 the different categories of information that he provided in connection with the different services.

13 298. Google therefore intentionally misrepresented the ability of Plaintiff Nisenbaum and
14 other members of the Android Device Switch Subclass to prevent the use of their personal
15 information for purposes other than those for which that information was originally provided. This
16 misrepresentation was made to induce Plaintiff Nisenbaum's, and the Android Device Switch
17 Subclass members', dependence on Google products and services, including Android and the
18 Android Market/Google Play, even while Google knew there was no simple and effective way for
19 users to prevent such data from being used in connection with other, non-Android products and
20 serves and for purposes of targeted advertising, so Google could enjoy substantial profits.

21 299. Google thereby violated Cal. Civ. Code § 1770(a)(9), (14), and (16).

22 300. As a result of Google's aggregation of his Android-related information with his non-
23 Android related information, Plaintiff Nisenbaum felt that his privacy interests were invaded and
24 purchased an alternative, non-Android mobile device in or about May 2012.

25 301. Plaintiff Nisenbaum would not have purchased an Android device in 2010 if Google
26 had disclosed that it would begin aggregating the information it collected in connection with Plaintiff
27 Nisenbaum's use of the device, including his use of the Android Market/Google Play, with
28

information Plaintiff Nisenbaum provided in connection with other Google products, including Gmail.

302. Further, as described above (see Counts I and II), Google intentionally misrepresented in advertisements making use of Android users' personal and proprietary data, including such users' names, images, and/or likenesses, that advertised goods and/or services have sponsorship or approval that they do not have, insofar as each users' endorsements were unauthorized, in violation of Cal. Civ. Code § 1770(a)(5).

303. Google's misappropriation of Android users' likenesses deprived such users of their financial interests in their own likenesses, in an amount to be proven at trial.

304. Plaintiff Nisenbaum and the members of the Android Device Switch Subclass are "consumers" within the meaning of Cal. Civ. Code § 1761(d) insofar as Plaintiff Nisenbaum and the members of the Android Device Switch Subclass acquired, by purchase or lease, Android-powered devices.

305. On March 29, 2012, a CLRA notice letter complying in all respects with Cal. Civ. Code § 1782(a) was served on Google. Plaintiff Anderson sent Google a letter via certified mail, return receipt requested, advising Google that it is in violation of the CLRA and demanding that it cease and desist from such violation, and make full restitution by refunding the monies received therefrom. Google was further advised that in the event that the relief requested has not been provided within thirty (30) days, Plaintiff Anderson would amend his complaint to include a request for monetary damages pursuant to the CLRA. That 30-day period having passed, Plaintiffs now include such a request. A true and correct copy of Plaintiff Anderson's CLRA letter is attached hereto as Exhibit A.

COUNT VII

VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code § 17200 *et seq.*

(On Behalf Of The Android App Disclosure Subclass)

306. Plaintiffs reallege and incorporate by reference each and every allegation set forth

1 above as though fully set forth herein.

2 307. Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough are Android
3 device users that have downloaded at least one Android application through Google Play.

4 308. Google violates the "fraudulent" prong of the UCL by intentionally and knowingly
5 misrepresenting that it will not disclose Android users' personal information, including the names,
6 email addresses, and physical or geographical locations of Plaintiffs Marti, DeMars, Barrios,
7 Anderson, Villani, and McCullough and the members of the Android App Disclosure Subclass, with
8 any third party without such users' consent.

9 309. In fact, Google does disclose such users' personal information, including the names,
10 email addresses, and physical or geographical locations of Plaintiffs Marti, DeMars, Barrios,
11 Anderson, Villani, and McCullough and the members of the Android App Disclosure Subclass, with
12 third-party application developers, each time they download and/or purchase an Android application
13 through Google Play – without obtaining their consent or authorization for such disclosure, and
14 without notifying them that such disclosure is being made.

15 310. Google represents that it does not disclose Android users' personal information to
16 third parties with the intent of inducing people to purchase Android devices and of inducing Android
17 users to register for, and to use, its products and services, including Google Play, and to download
18 applications through Google Play. Google does so even while knowing that there is no meaningful
19 way to prevent one's name, email address, and physical or geographical location from being
20 disclosed to third-party application developers, as long as applications are downloaded and/or
21 purchased by the user.

22 311. Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough and the
23 members of the Android App Disclosure Subclass justifiably relied upon those misrepresentations
24 when deciding to use Google Play and to download and/or purchase Android applications.

25 312. Each time Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough
26 downloaded and/or purchased Android applications, Google caused their personal information to be
27 transmitted from their Android devices to the developer or developers of the applications
28

downloaded, thus consuming finite resources purchased by Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough, including device battery power and bandwidth.

313. Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough and the members of the Android App Disclosure Subclass suffered damages in the form of consumed device battery power and bandwidth, as alleged above, in an amount to be proven at trial.

314. Google violated the "unfair" prong of the UCL by leading Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough and the members of the Android App Disclosure Subclass to believe that their personal information would be withheld from all third parties, encouraging Plaintiffs and the members of the Android App Disclosure Subclass to make Android devices and applications indispensable to their lives, and then secretly using Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough's and the Android App Disclosure Subclass members' personal information in a manner in which Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough and the Android App Disclosure Subclass members did not and would not agree, and in a manner from which they cannot effectively opt out.

315. Google's unfair, deceptive, and fraudulent practices originated from California. In addition, decisions concerning Google's privacy policies, including decisions about the surreptitious and involuntary disclosure of Android users' personal information, were made in California.

316. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough and the members of the Android App Disclosure Subclass seek an order from this Court permanently enjoining Google from continuing to engage in the unlawful, unfair, and fraudulent conduct described herein. Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough and the Android App Disclosure Subclass seek an order requiring Google to (1) immediately cease the unlawful practices described in this Complaint; and (2) award Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough and the Android App Disclosure Subclass reasonable costs and attorneys' fees pursuant to Cal. Code of Civ. Proc. § 1021.5.

317. Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough and the Android App Disclosure Subclass members have expended funds in acquiring the resources

necessary to transmit their personal information from their Android devices to third-party application developers, including the costs of powering their Android devices and of acquiring internet access and bandwidth for their Android devices, and Google has deprived them of these funds by automatically and nonconsensually causing their devices to report such information to third-party application developers.

318. In addition, Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough and the Android App Disclosure Subclass members are each subject to an increased, unexpected, and unreasonable risk to their personal information, including risks of further invasions of privacy, and of harassment, identity theft, and other security events, thanks to Google's practice of disclosing to third-party app developers their personal information in every Play transaction.

COUNT VIII

BREACH OF CONTRACT

(On Behalf Of The Android App Disclosure Subclass)

319. Plaintiffs reallege and incorporate by reference each and every allegation set forth above as though fully set forth herein.

320. In connection with their registration of an account for use on their Android devices and on Google Play, Google represented that it would "ask for [Plaintiff Marti's, DeMars', Barrios', Anderson's, Villani's, and McCullough's] consent prior to" any use "different than the purpose for which [the information collected in connection with Plaintiff Marti's, DeMars', Barrios', Anderson's, Villani's, and McCullough's use of their Android devices] was collected."

321. Further, the new unified privacy policy states that Google "will share personal information with companies, organizations or individuals outside of Google when we have your consent to do so."

322. The new privacy policy provides a limited universe of exceptions to this rule, none of which pertain to the disclosure of Android users' personal information to third-party application developers.

323. Google breached its contract with Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough, and the members of the Android App Disclosure Subclass, when it began to disclose personal information belonging to Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough and Android App Disclosure Subclass members to third-party application developers.

324. Google further breached its contract with Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough and the members of the Android App Disclosure Subclass by failing to obtain their consent for such disclosure.

325. As a result of Google's breach of its contract with Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough and the members of the Android App Disclosure Subclass, those Plaintiffs and Android App Disclosure Subclass members have suffered and will continue to suffer damages in the form of the costs each has paid to acquire the resources necessary to transmit their personal information from their Android devices to third-party application developers, including the costs of charging their Android devices and of acquiring internet access and bandwidth for their Android devices.

326. Google has deprived them of these funds by automatically and nonconsensually causing their devices to report such information to third-party application developers, in violation of the terms governing the contracts between Google and Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough and all members of the Android App Disclosure Subclass.

327. In addition, Plaintiffs Marti, DeMars, Barrios, Anderson, Villani, and McCullough and the Android App Disclosure Subclass members are each subject to an increased, unexpected, and unreasonable risk to their personal information, including risks of further invasions of privacy, and of harassment, identity theft, and other security events, thanks to Google's practice of disclosing to third-party app developers their personal information in every Play transaction.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

COUNT IX

VIOLATIONS OF THE FEDERAL WIRETAP ACT

18 U.S.C. § 2511

(On Behalf Of The Class)

328. Plaintiffs reallege and incorporate by reference each and every allegation set forth above as though fully set forth herein.

329. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of any wire, oral or electronic communication through use of a device.

330. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral, or electronic communication is intercepted through use of a device.

331. Through its use of computer systems, applications, and/or code unrelated to the provision of the Gmail service, Google is intercepting the contents of Plaintiffs' electronic communications on Gmail by scanning the contents of such communications, including without limitation communications sent to Plaintiffs and en route to their destinations in Plaintiffs' e-mailboxes as well as communications sent by Plaintiffs and en route to their destinations in other users' e-mailboxes, in order to provide targeted advertisements within the Gmail service. Such scanning occurs contemporaneously with the transmission of Gmail communications.

332. Through its use of computer systems, applications, and/or code unrelated to the provision of the Gmail service, Google is also intercepting the contents of Plaintiffs' electronic communications on Gmail by scanning the contents of such communications and disclosing the contents of such communications to services other than Gmail, including without limitation Google+, YouTube, Picasa, Maps, Docs, Reader, google.com search, Voice, and others, in order to provide targeted advertisements on those services and on third-party sites that have partnered with Google in an advertising network. Such scanning and disclosure occurs contemporaneously with the transmission of Gmail communications.

333. Through its use of computer systems, applications, and/or code unrelated to the provision of the Gmail service, Google is also intercepting the contents of Plaintiffs' electronic communications on Gmail by scanning the contents of such communications and disclosing the contents of such communications to independent, unidentified third-party entities that Google has engaged. Such scanning and disclosure occurs contemporaneously with the transmission of Gmail communications.

334. Neither Plaintiffs nor members of the Class consented, nor were they aware that Google was violating its own privacy policy, and tracking and aggregating consumers' internet use across Google platforms, creating a single profile of each consumer that aggregates all information about the consumer across Google platforms – even after logging off of Google accounts – and then appending the aggregated information to consumers' Google accounts when they log back in.

335. The data Google is intercepting and aggregating, which include the contents of Gmail messages and contact lists, are "communications" within the meaning of the Wiretap Act.

336. Google intentionally and willfully intercepts the electronic communications of its consumers and intentionally and willfully aggregates consumers' personal information for its own financial benefit pursuant to the new privacy policy introduced on March 1, 2012.

337. The independent, unidentified third-party entities to which Google exposes Plaintiffs' electronic communications are engaged not to deliver the Gmail service but to facilitate the targeting of advertisements to Plaintiffs.

338. Plaintiffs are persons whose electronic communications were intercepted within the meaning of Section 2520.

339. Section 2520 provides for preliminary, equitable and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 a day for each day of violation, actual and punitive damages, reasonable attorneys' fees, and disgorgement of any profits earned by Google as a result of the above-described violations.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

COUNT X

VIOLATIONS OF THE STORED ELECTRONIC COMMUNICATIONS ACT

18 U.S.C. § 2701

(On Behalf Of The Class)

340. Plaintiffs reallege and incorporate by reference each and every allegation set forth above as though fully set forth herein.

341. The Stored Electronic Communications Act ("SECA") provides a cause of action against a person who intentionally accesses without authorization a facility through which an electronic communication service is provided, or who intentionally exceeds an authorization to access that facility and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in storage in such a system.

342. "Electronic Storage" is defined in the statute to include "any temporary, immediate storage of a wire or electronic communication incidental to the electronic transmission thereof."

343. Google's new privacy policy intentionally exceeds its authorized access to consumers' electronic communications stored on Google's systems, including without limitation Plaintiffs' Gmail messages and contact lists, thus violating the SECA.

344. Pursuant to its new privacy policy, Google also discloses the contents of Plaintiffs' and other consumers' electronic communications, including without limitation Plaintiffs' Gmail messages and contact lists, to other services or products to which no Plaintiff gave authorization to access such communications, thus violating the SECA.

345. Google also intentionally places cookies on consumers' computers that access members' stored electronic communications without authorization, thus violating the SECA.

346. Further, Google engages independent, unidentified third-party entities to process and distribute user information across its product platforms, including the contents of Plaintiffs' Gmail communications. Such third parties are thus exposed to Plaintiffs' electronic communications, without Plaintiffs' authorization.

1 347. Plaintiffs and the other Class members were, and continue to be, harmed by Google's
2 violations, and are entitled to statutory, actual and compensatory damages, injunctive relief, punitive
3 damages and reasonable attorneys' fees.

4 **PRAYER FOR RELIEF**

5 WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray the
6 Court to enter judgment against Google and in favor of Plaintiffs, on behalf of themselves and the
7 Class members, and to award the following relief:

8 A. Certifying this action as a nationwide class action, certifying Plaintiffs as
9 representatives of the Class, and designating their counsel as counsel for the Class;

10 B. Tolling the statute of limitations pursuant to the discovery rule and the doctrine of
11 fraudulent concealment;

12 C. Awarding the Plaintiffs and each Class member actual and compensatory damages for
13 the acts complained of herein;

14 D. Awarding the Plaintiffs and each Class member treble damages for the acts
15 complained of herein, where permitted by law;

16 E. Awarding the Plaintiffs and each Class member costs of suit and attorneys' fees, as
17 allowed by law, and/or awarding counsel for the Class attorneys' fees;

18 F. Awarding the Plaintiffs and each Class member statutory pre-judgment interest;

19 G. Awarding legal and equitable relief as this Court may deem just and proper; and

20 H. Granting such other or further relief as may be appropriate under the circumstances.

21 **DEMAND FOR JURY TRIAL**

22 Plaintiffs demand a trial by jury as to all issues so triable.

23 Dated: March 7, 2013 **BURSOR & FISHER, P.A.**

24 By: */s/ L. Timothy Fisher*

25 L. Timothy Fisher (State Bar No. 191626)
Sarah N. Westcot (State Bar No. 264916)
26 1990 North California Boulevard, Suite 940
Walnut Creek, California 94596
27 Tel: 925-300-4455
Fax: 925-407-2700

28

GARDY & NOTIS, LLP
Mark C. Gardy
James S. Notis *(pro hac vice)*
Kelly A. Noto *(pro hac vice)*
Charles A. Germershausen
560 Sylvan Avenue
Englewood Cliffs, New Jersey 07632
Tel: 201-567-7377
Fax: 201-567-7337

GRANT & EISENHOFER P.A.
James J. Sabella *(pro hac vice)*
Diane Zilka *(pro hac vice)*
Kyle McGee *(pro hac vice)*
485 Lexington Avenue, 29th Floor
New York, New York 10017
Tel: 646-722-8500
Fax: 646-722-8501

Interim Lead Counsel for the Class

CARELLA, BYRNE, CECCHI OLSTEIN, BRODY & AGNELLO
James E. Cecchi
5 Becker Farm Road
Roseland, New Jersey 07068
Tel: 973-994-1700
Fax: 973-994-1744

LAW OFFICES OF RICHARD S. SCHIFFRIN LLC
Richard S. Schiffrin
P.O. Box 2258
West Chester, Pennsylvania 19380
Tel: 610-203-7154

JAMES SCHWARTZ & ASSOCIATES PC
Michael Schwartz
1500 Walnut Street, 21st Floor
Philadelphia, Pennsylvania 19102
Tel: 215-751-9865
Fax: 215-751-0658

LAW OFFICES OF MARTIN S. BAKST
Martin S. Bakst (65112)
15760 Ventura Boulevard, Sixteenth Floor
Encino, California 91436
Tel: 818-981-1400
Fax: 818-981-5550

Of Counsel for the Class

EXHIBIT A

1990 N. CALIFORNIA BLVD
WALNUT CREEK, CA 94596
www.bursor.com

SARAH N. WESTCOT
TEL: 925.300.4455
FAX: 925.407.2700
swestcot@bursor.com

March 29, 2012

Via Certified Mail – Return Receipt Requested

Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Re: Demand Letter Pursuant to California Civil Code § 1782

To Whom It May Concern:

This letter serves as a preliminary notice and demand for corrective action by Google Inc. ("Google") pursuant to the provisions of California Civil Code § 1782, on behalf of our client, Nicholas Anderson, and all other persons similarly situated.

On March 1, 2012, Google implemented a new Privacy Policy that allows it to consolidate user data across dozens of Google services, including Google Search, Gmail, YouTube, Google+, and AdSense. For example, from within Youtube, Google can now access users' search histories from Google Search, browsing habits from AdSense, and social networking data from Google+. Previously, Google did not consolidate its user data across its services. Each service kept its own records of users' activities. Users expected this level of privacy when they signed up for Google services prior to March 1, 2012.

Google has engaged in a uniform marketing and advertising program representing that its new Privacy Policy — and the decision to consolidate user data — was implemented for the sake of simplicity and to improve users' experiences on Google services. These representations were prominently displayed on Google's Official Blog, Google's Good to Know advertising campaign, and in an open letter to eight Congressional representatives.

However, Google misled consumers because it failed to highlight its true goal: consolidating user data for advertising purposes. Writers, technology experts, and even a former Google Engineering Director recognize that the new Privacy Policy is intended to help Google place targeted advertisements. Advertisers are willing to pay a premium to advertise with Google because it has this user data.

Google's previous privacy policies prohibit the consolidation of user data. Users did not agree to have Google consolidate their user data for advertising. Users did not agree to share this information across Google's dozens of different services. There is no simple and effective way to opt out; users must manage their privacy settings in each Google service.

If a computer user disagrees with Google's new Privacy Policy, the remedy is to stop using his or her Google Account. But terminating a Google Account is time-consuming, inconvenient, and costly. Users may have Google Accounts for email, advertising, webpage analytics, or other purposes. A loss of a Google Account means a loss of business, advertising, and opportunity.

Users with Android phones are in the worst position. Google connectivity is heavily integrated into these devices. Google connectivity is used for email, chat, and purchasing content. If an Android user disagrees with the change, the only remedy is to discard the phone or cease using smartphone functionality.

Nicholas Anderson is a citizen of the State of California and is a consumer as defined in California Civil Code §1761(d) in that he purchased an Android phone and has a Google account "for personal, family or household purposes." At the time of purchase, Mr. Anderson was familiar with Google's existing privacy policies, and he relied on such misrepresentations in deciding to purchase his Android phone.

Mr. Anderson would not have purchased an Android phone if he had known that Google would breach its existing privacy policies by consolidating his user data. Mr. Anderson suffered a loss of money as a result of Google's misrepresentation in the amount of the purchase price of his Android phone.

By misrepresenting its existing privacy policies and misrepresenting the reasons for consolidating user data, Google has violated numerous provisions of California law including the Consumers Legal Remedies Act, Civil Code § 1770, including but not limited to subsections (a)(9), (14), and (16).

We hereby demand that Google immediately (1) abide by the terms of its privacy policies prior to March 1, 2012; (2) remove consolidated user data from its possession; (3) adequately disclose that advertising considerations were a material factor in Google's decision to consolidate user data; (4) cease using consolidated user data to deliver targeted advertisements; and (5) agree that it will only consolidate user data on a purely opt-in basis.

It is further demanded that Google preserve all documents and other evidence which refer or relate to any of the above-described practices including, but not limited to, the following:

1. All documents concerning the development and implementation of consolidating user data;

2. All communications with advertisers and marketing affiliates concerning the potential uses of consolidated user data;

3. All documents comparing Google's user data to the data held by its competitors, including Facebook; and

4. All communications with customers concerning complaints or comments relating to consolidated user data.

Please comply with this demand within 30 days from receipt of this letter. If the relief requested has not been provided within 30 days from receipt of this letter, Plaintiff will amend the Complaint to include a request for monetary damages pursuant to the CLRA.

We are willing to negotiate with Google to attempt to resolve the demands asserted in this letter. If Google wishes to enter into such discussions, please contact me immediately.

If Google contends that any statement in this letter is inaccurate in any respect, please provide us with your contentions and supporting documents immediately upon receipt of this letter, but in no event later than 30 days from the date of receipt.

Very truly yours,

Sarah N. Westcot