

1 SPECTOR ROSEMAN KODROFF & WILLS, PC
Jeffrey L. Kodroff, Esq.
2 1818 Market St., Ste. 2500
Philadelphia, PA 19103
3 Tel. 215-496-0300
Fax. 215-496-6611
4

5 COHEN MILSTEIN SELLERS & TOLL PLLC
Daniel A. Small, Esq.
1100 New York Avenue, NW, Suite 500W
6 Washington, DC 20005
Tel. 202-408-4600
7 Fax. 202-408-4699

8 *Plaintiff Co-Lead Counsel*

9 LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Elizabeth J. Cabraser, Esq.
10 275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
11 Tel. 415-956-1000
Fax. 415-956-1008
12

13 *Plaintiffs' Liaison Counsel*

14 UNITED STATES DISTRICT COURT
15 NORTHERN DISTRICT OF CALIFORNIA
16 SAN JOSE DIVISION
17

18 IN RE: GOOGLE, INC. STREET VIEW
ELECTRONIC COMMUNICATIONS
19 LITIGATION

No. 5:10-md-02184 JW

**CONSOLIDATED
CLASS ACTION COMPLAINT**

JURY TRIAL DEMANDED

22
23 Plaintiffs Patrick Keyes, Matthew Berlage, Aaron Linsky, James Fairbanks, Jeffrey
24 Colman, John Redstone, Karl Schulz, Dean Bastilla, Vicki Van Valin, Stephanie and Russell
25 Carter, Danielle Reyas, Bertha Davis, Jason Taylor, Jennifer Locsin, James Blackwell, Rich
26 Benitti, Benjamin Joffe, Lilla Marigza, Wesley Hartline, David Binkley, and Eric Myhre
27 (collectively, "Plaintiffs"), individually and on behalf of a Class (defined below) of all others
28 similarly situated, bring this action for damages and declaratory and injunctive relief under

1 Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (also known as the Wiretap
2 Act), as amended by the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511, *et*
3 *seq.*, various state wiretap statutes, and the California Business and Professional Code § 17200, *et*
4 *seq.* against Defendant Google, Inc. (“Defendant”), and demand a jury trial.

5 **I. NATURE OF THE CASE**

6 1. Defendant intentionally intercepted electronic communications sent or received on
7 wireless internet connections (“WiFi connections”) by the Class from at least May 25, 2007
8 through the present in violation of the Wiretap Act and related state statutes. Defendant also
9 misrepresented the nature of its Street View service. While Defendant told the general public it
10 was collecting and displaying images only, in fact, Defendant was also secretly gathering
11 personal data received and sent over privately owned, individual WiFi connections.

12 2. Defendant intercepted the Class members’ electronic communications with its
13 Google Street View vehicles. Google Street View is a web-based and web-accessed technology
14 featured in Google Maps and Google Earth that displays images taken from a fleet of specially
15 adapted cars, known as Google Street Vehicles, and provides panoramic views of homes, offices
16 and other buildings to users from various positions along many streets world-wide. Defendant
17 launched Google Street View on May 25, 2007 in the United States, and has since expanded this
18 offering to more than 30 nations.

19 3. Unbeknownst to Google Street View users and the general public, Defendant also
20 used Google Street View vehicles not just to collect images for inclusion on Google Maps and
21 Google Earth, but for other, secret purposes.

22 4. When Defendant’s engineers created the data collection system for its Google
23 Street View vehicles, most commonly known as a packet analyzer or wireless sniffer, they
24 intentionally included computer code in the system that was designed to and did sample, collect,
25 decode, and analyze all types of data sent and received over the WiFi connections of Class
26 members. This data included Class members’ unique, secret WiFi network identifiers (known as
27 Service Set Identifier or SSID) and unique WiFi router numbers (Media Access Control or MAC
28 addresses). The data also included all or part of any personal emails, passwords, videos, audio,

1 documents, and Voice Over Internet Protocol (“VOIP”) information (collectively, “payload
2 data”) transmitted over Class members’ WiFi networks in which plaintiffs had a reasonable
3 expectation of privacy. The employment of packet sniffers, and thus the underlying code, was
4 approved by Defendant’s project team leaders before it was included in the Google Street View
5 vehicles.

6 5. The WiFi networks from which the Google Street View vehicles collected payload
7 data were not configured so that such data were reasonably accessible by the general public.
8 Indeed, the data, as captured by the wireless sniffer, are not even readable by members of the
9 public absent use of sophisticated decoding and processing technology. Plaintiffs did not give
10 their consent to Defendant to collect these data, nor did they have knowledge that Google Street
11 View vehicles had been collecting these data.

12 6. After the Google Street View vehicles’ wireless sniffers sampled, collected, and
13 decoded these data, Defendant stored the data on its servers. Defendant has admitted that it has
14 collected and stored data from WiFi connections around the world, including the United States.
15 At present, data gathered in the United States has been ordered preserved by a federal court.
16 Pursuant to a motion for a temporary restraining order in *Van Valin, et al. v. Google Inc.*, 3:10-cv-
17 0057-MO (D. Or. filed May 17, 2010), Judge Mosmon issued an Order dated May 24, 2010
18 requiring Google to “Produce two exact bit-by-bit mirror image copies of the existing hard drive
19 (described by the Defendant as an encrypted hard drive containing the ‘payload’ data for the
20 United States), such that upon completion of the process, the target disks are identical to and
21 interchangeable with the existing source disk (‘clones’).”

22 7. Yet Defendant’s startling admission came not several years ago—when Defendant
23 first began collecting and storing the data—but only very recently, on May 14, 2010. This
24 admission surfaced in the course of an audit of Defendant’s data collection operations that
25 German data protection authorities recently initiated in light of privacy concerns.

26 8. Defendant’s high-level officials have since admitted that Google collected and
27 stored Class members’ WiFi data, including payload data. Google has also admitted that it
28

1 included code in Google Street View vehicles' data collection systems that its engineers knew
2 would intercept Class members' payload data.

3 9. On May 19, 2010, German prosecutors based in Hamburg announced the opening
4 of a criminal investigation into Defendant's conduct. Data protection agencies in Italy, Spain,
5 and France announced the same day that they too had opened investigations into Defendant's
6 activities. And the Czech Republic has been looking into Google Street View since April 2010.

7 10. Australia's minister for broadband, communications, and the digital economy,
8 Stephen Conroy, has told an Australian senate committee that Defendant deliberately decided to
9 collect payload data. Conroy also said that Defendant's claims that it collected data by mistake
10 were wrong, and that Defendant deliberately wrote a computer code designed to gather the private
11 information.

12 11. Most recently, U.K. authorities concluded that Google's actions violated U.K. data
13 protection law. U.K. Information Commissioner Christopher Graham said Google's actions
14 constituted a "significant breach" of data protection law. Mr. Graham added that his office would
15 ask Google to sign a binding commitment to prevent future breaches and agree to an audit of its
16 data protection practices in the U.K.

17 <http://online.wsj.com/article/SB10001424052748703506904575591963217799010.html?mod=W>
18 [SJ_hp_MIDDLENexttoWhatsNewsForth](#).

19 12. The alarm and outcry over Defendant's conduct has not been limited to overseas.
20 United States Congressmen have requested governmental investigation into Defendant's conduct.
21 In addition, many State Attorney General's offices have announced that they are investigating the
22 matter.

23 13. Multiple private actions have also been brought on behalf of individuals who
24 allege that their private data was stolen by Google. These cases have been consolidated for pre-
25 trial purposes in this Court.

26 14. As a result of Defendant's unlawful conduct, Plaintiffs, on behalf of themselves
27 and members of the Class, bring this action to recover statutory damages, punitive damages,
28

1 equitable relief, and attorneys' fees and costs under 18 U.S.C. § 2520, the California Business and
2 Professional Code § 17200, *et seq.*, and various state wiretap statutes as described below.

3 **II. JURISDICTION AND VENUE**

4 15. This Court has jurisdiction under 28 U.S.C. § 1331 because Plaintiffs have alleged
5 the violation of a federal statute, 18 U.S.C. § 2511, *et seq.* This Court may also exercise
6 supplemental jurisdiction over the state law claims plead below.

7 16. Venue lies within this District under 28 U.S.C. § 1391(b)-(c) because:

8 (a) Defendant conducts business in this District; (b) certain acts giving rise to the claims asserted
9 in this Complaint occurred in this District; (c) the actions of Defendant alleged in this Complaint
10 caused damage to certain of the Plaintiffs and a substantial number of Class members within this
11 District; and (d) Defendant maintains an office in this District.

12 17. Venue also lies within this District because the United States Judicial Panel on
13 Multidistrict Litigation centralized all related litigation to this court. *See* Transfer Order (JPML
14 Aug. 17, 2010).

15 **III. PARTIES**

16 **A. Plaintiffs**

17 18. Plaintiff Patrick Keyes is an individual who resides within and is a citizen of
18 Washington, D.C. During the class period, Mr. Keyes maintained and used a WiFi connection at
19 his home. Mr. Keyes used the WiFi connection to send and receive various types of private
20 payload data, including usernames, passwords, and personal emails. His network was not readily
21 accessible to the general public. Mr. Keyes's home can be seen on Google Maps and Street
22 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data
23 from Plaintiff's WiFi connection, including payload data, on at least one occasion. Mr. Keyes did
24 not know that Google collected his data, nor did he give permission for Google to do so.

25 19. Plaintiff Matthew Berlage is an individual who resides within and is a citizen of
26 Ohio. During the class period, Mr. Berlage maintained and used a WiFi connection at his home.
27 Mr. Berlage used the WiFi connection to send and receive various types of private payload data,
28 including usernames, passwords, and personal emails. His network was not readily accessible to

1 the general public. Mr. Berlage's home can be seen on Google Maps and Street View. On
2 information and belief, Defendant surreptitiously collected, decoded, and stored data from his
3 WiFi connection, including payload data, on at least one occasion. Mr. Berlage did not know that
4 Google collected his data, nor did he give permission for Google to do so.

5 20. Plaintiff Jeffrey Colman is an individual who resides within and is a citizen of
6 Washington, D.C. During the class period, Mr. Colman maintained and used a WiFi connection
7 at his home. Mr. Colman used the WiFi connection to send and receive various types of private
8 payload data, including usernames, passwords, and personal emails. His network was not readily
9 accessible to the general public. Mr. Colman's home can be seen on Google Maps and Street
10 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data
11 from his WiFi connection, including payload data, on at least one occasion. Mr. Colman did not
12 know that Google collected his data, nor did he give permission for Google to do so.

13 21. Plaintiffs Stephanie and Russell Carter are individuals who reside within and are
14 citizens of Pennsylvania. During the class period, Mr. and Mrs. Carter maintained and used a
15 WiFi connection at their home. Mr. and Mrs. Carter used the WiFi connection to send and
16 receive various types of private payload data, including usernames, passwords, and personal
17 emails. Their network was not readily accessible to the general public. Their home can be seen
18 on Google Maps and Street View. On information and belief, Defendant surreptitiously
19 collected, decoded, and stored data from their WiFi connection, including payload data, on at
20 least one occasion. Mr. and Mrs. Carter did not know that Google collected their data, nor did
21 they give permission for Google to do so.

22 22. Plaintiff Benjamin Joffe is an individual who resides within and is a citizen of
23 Nevada. During the class period, Mr. Joffe maintained and used a WiFi connection at his home.
24 Mr. Joffe used the WiFi connection to send and receive various types of private payload data,
25 including usernames, passwords, and personal emails. His network was not readily accessible to
26 the general public. Mr. Joffe's home can be seen on Google Maps and Street View. On
27 information and belief, Defendant surreptitiously collected, decoded, and stored data from his
28

1 WiFi connection, including payload data, on at least one occasion. Mr. Joffe did not know that
2 Google collected his data, nor did he give permission for Google to do so.

3 23. Plaintiff Wesley Hartline is an individual who resides within and is a citizen of
4 Tennessee. During the class period, Mr. Hartline maintained and used a WiFi connection at his
5 home. Mr. Hartline used the WiFi connection to send and receive various types of private
6 payload data, including usernames, passwords, and personal emails. His network was not readily
7 accessible to the general public. Mr. Hartline's home can be seen on Google Maps and Street
8 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data
9 from his WiFi connection, including payload data, on at least one occasion. Mr. Hartline did not
10 know that Google collected his data, nor did he give permission for Google to do so.

11 24. Plaintiff David Binkley is an individual who resides within and is a citizen of
12 Tennessee. During the class period, Mr. Binkley maintained and used a WiFi connection at his
13 home. Mr. Binkley used the WiFi connection to send and receive various types of private
14 payload data, including usernames, passwords, and personal emails. His network was not readily
15 accessible to the general public. Mr. Binkley's home can be seen on Google Maps and Street
16 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data
17 from his WiFi connection, including payload data, on at least one occasion. Mr. Binkley did not
18 know that Google collected his data, nor did he give permission for Google to do so.

19 25. Plaintiff Eric Myhre is an individual who resides within and is a citizen of
20 Washington. During the class period, Mr. Myhre maintained and used a WiFi connection at his
21 home. Mr. Myhre used the WiFi connection to send and receive various types of private payload
22 data, including usernames, passwords, and personal emails. His network was not readily
23 accessible to the general public. Mr. Myhre's home can be seen on Google Maps and Street
24 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data
25 from his WiFi connection, including payload data, on at least one occasion. Mr. Myhre did not
26 know that Google collected his data, nor did he give permission for Google to do so.

27 26. Plaintiff Aaron Linskey is an individual who resides within and is a citizen of
28 California. During the class period, Mr. Linskey maintained and used a WiFi connection at his

1 home. Mr. Linskey used the WiFi connection to send and receive various types of private
2 payload data, including usernames, passwords, and personal emails. His network was not readily
3 accessible to the general public. Mr. Linskey's home can be seen on Google Maps and Street
4 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data
5 from his WiFi connection, including payload data, on at least one occasion. Mr. Linskey did not
6 know that Google collected his data, nor did he give permission for Google to do so.

7 27. Plaintiff James Fairbanks is an individual who resides within and is a citizen of
8 California. During the class period, Mr. Fairbanks maintained and used a WiFi connection at his
9 home. Mr. Fairbanks used the WiFi connection to send and receive various types of private
10 payload data, including usernames, passwords, and personal emails. His network was not readily
11 accessible to the general public. Mr. Fairbank's home can be seen on Google Maps and Street
12 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data
13 from his WiFi connection, including payload data, on at least one occasion. Mr. Fairbanks did
14 not know that Google collected his data, nor did he give permission for Google to do so.

15 28. Plaintiff John Redstone is an individual who resides within and is a citizen of
16 Illinois. During the class period, Mr. Redstone maintained and used a WiFi connection at his
17 home. Mr. Redstone used the WiFi connection to send and receive various types of private
18 payload data, including usernames, passwords, and personal emails. His network was not readily
19 accessible to the general public. Mr. Redstone's home can be seen on Google Maps and Street
20 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data
21 from his WiFi connection, including payload data, on at least one occasion. Mr. Redstone did not
22 know that Google collected his data, nor did he give permission for Google to do so.

23 29. Plaintiff Karl Schulz is an individual who resides within and is a citizen of Illinois.
24 During the class period, Mr. Schulz maintained and used a WiFi connection at his home. Mr.
25 Schulz used the WiFi connection to send and receive various types of private payload data,
26 including usernames, passwords, and personal emails. His network was not readily accessible to
27 the general public. Mr. Schulz's home can be seen on Google Maps and Street View. On
28 information and belief, Defendant surreptitiously collected, decoded, and stored data from his

1 WiFi connection, including payload data, on at least one occasion. Mr. Schulz did not know that
2 Google collected his data, nor did he give permission for Google to do so.

3 30. Plaintiff Dean Bastilla is an individual who resides within and is a citizen of
4 Illinois. During the class period, Mr. Bastilla maintained and used a WiFi connection at his
5 home. Mr. Bastilla used the WiFi connection to send and receive various types of private payload
6 data, including usernames, passwords, and personal emails. His network was not readily
7 accessible to the general public. Mr. Bastilla's home can be seen on Google Maps and Street
8 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data
9 from his WiFi connection, including payload data, on at least one occasion. Mr. Bastilla did not
10 know that Google collected his data, nor did he give permission for Google to do so.

11 31. Plaintiff Van Valin is an individual who resides within and is a citizen of Oregon.
12 During the class period, Mr. Van Valin maintained and used a WiFi connection at his home. Mr.
13 Van Valin used the WiFi connection to send and receive various types of private payload data,
14 including usernames, passwords, and personal emails. His network was not readily accessible to
15 the general public. Mr. Van Valin's home can be seen on Google Maps and Street View. On
16 information and belief, Defendant surreptitiously collected, decoded, and stored data from his
17 WiFi connection, including payload data, on at least one occasion. Mr. Van Valin did not know
18 that Google collected his data, nor did he give permission for Google to do so.

19 32. Plaintiff Danielle Reyas is an individual who resides within and is a citizen of
20 California. During the class period, Ms. Reyas maintained and used a WiFi connection at her
21 home. Ms. Reyas used the WiFi connection to send and receive various types of private payload
22 data, including usernames, passwords, and personal emails. Her network was not readily
23 accessible to the general public. Ms. Reyas's home can be seen on Google Maps and Street
24 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data
25 from her WiFi connection, including payload data, on at least one occasion. Ms. Reyas did not
26 know that Google collected her data, nor did she give permission for Google to do so.

27 33. Plaintiff Bertha Davis is an individual who resides within and is a citizen of
28 California. During the class period, Ms. Davis maintained and used a WiFi connection at her

1 home. Ms. Davis used the WiFi connection to send and receive various types of private payload
2 data, including usernames, passwords, and personal emails. Her network was not readily
3 accessible to the general public. Ms. Davis's home can be seen on Google Maps and Street View.
4 On information and belief, Defendant surreptitiously collected, decoded, and stored data from her
5 WiFi connection, including payload data, on at least one occasion. Ms. Davis did not know that
6 Google collected her data, nor did she give permission for Google to do so.

7 34. Plaintiff Jason Taylor is an individual who resides within and is a citizen of
8 California. During the class period, Mr. Taylor maintained and used a WiFi connection at his
9 home. Mr. Taylor used the WiFi connection to send and receive various types of private payload
10 data, including usernames, passwords, and personal emails. His network was not readily
11 accessible to the general public. Mr. Taylor's home can be seen on Google Maps and Street
12 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data
13 from his WiFi connection, including payload data, on at least one occasion. Mr. Taylor did not
14 know that Google collected his data, nor did he give permission for Google to do so.

15 35. Plaintiff Jennifer Locsin is an individual who resides within and is a citizen of
16 California. During the class period, Ms. Locsin maintained and used a WiFi connection at her
17 home. Ms. Locsin used the WiFi connection to send and receive various types of private payload
18 data, including usernames, passwords, and personal emails. Her network was not readily
19 accessible to the general public. Ms. Locsin's home can be seen on Google Maps and Street
20 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data
21 from her WiFi connection, including payload data, on at least one occasion. Ms. Locsin did not
22 know that Google collected her data, nor did she give permission for Google to do so.

23 36. Plaintiff James Blackwell is an individual who resides within and is a citizen of
24 California. During the class period, Mr. Blackwell maintained and used a WiFi connection at his
25 home. Mr. Blackwell used the WiFi connection to send and receive various types of private
26 payload data, including usernames, passwords, and personal emails. His network was not readily
27 accessible to the general public. Mr. Blackwell's home can be seen on Google Maps and Street
28 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data

1 from his WiFi connection, including payload data, on at least one occasion. Mr. Blackwell did
2 not know that Google collected his data, nor did he give permission for Google to do so.

3 37. Plaintiff Ric Benitti is an individual who resides within and is a citizen of
4 California. During the class period, Mr. Benitti maintained and used a WiFi connection at his
5 home. Mr. Benitti used the WiFi connection to send and receive various types of private payload
6 data, including usernames, passwords, and personal emails. His network was not readily
7 accessible to the general public. Mr. Benitti's home can be seen on Google Maps and Street
8 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data
9 from his WiFi connection, including payload data, on at least one occasion. Mr. Benitti did not
10 know that Google collected his data, nor did he give permission for Google to do so.

11 38. Plaintiff Lilla Marigza is an individual who resides within and is a citizen of
12 Tennessee. During the class period, Ms. Marigza maintained and used a WiFi connection at her
13 home. Ms. Marigza used the WiFi connection to send and receive various types of private
14 payload data, including usernames, passwords, and personal emails. Her network was not readily
15 accessible to the general public. Ms. Marigza's home can be seen on Google Maps and Street
16 View. On information and belief, Defendant surreptitiously collected, decoded, and stored data
17 from her WiFi connection, including payload data, on at least one occasion. Ms. Marigza did not
18 know that Google collected her data, nor did she give permission for Google to do so.

19 **B. Defendant**

20 39. Defendant Google, Inc. ("Defendant") is a Delaware corporation with its principal
21 place of business in Mountain View, California. Defendant compiles information and makes it
22 searchable via the Internet. It develops and hosts numerous Internet-based services and products.
23 Defendant posted a \$6.5 billion profit in 2009, making it the world's 19th most profitable
24 company according to *Fortune* magazine.

25 **IV. FACTUAL ALLEGATIONS**

26 **A. Defendant's Business And Culture**

27 40. Defendant states on its website that its name "reflects the immense volume of
28 information that exists, and the scope of [its] mission: to organize the world's information and

1 make it universally accessible and useful.” Defendant also boasts on its website of its “superior
2 search technology,” and that “[a]s with its technology, [it] has chosen to ignore conventional
3 wisdom in designing its business.”

4 41. Defendant is widely recognized to employ some of the best and brightest
5 individuals in the high-technology industry. On its website section titled “Google Management,”
6 Defendant lays claim to “a management team that represents some of the most experienced
7 technology professionals in the industry.”

8 42. Defendant at the same time recognizes the importance and value of its lower level
9 employees’ contributions to its business operations. On its website section titled “Google
10 Culture,” Defendant provides: “Every employee is a hands-on contributor, and everyone wears
11 several hats. Because we believe that each Googler is an equally important part of our success,
12 no one hesitates to pose questions directly to [co-founders] Larry [Page] or Sergey [Brin] in our
13 weekly all-hands (“TGIF”) meetings.”

14 43. Moreso than other companies, even including those in the high-technology sector,
15 engineers play a pivotal and ubiquitous role in Defendant’s daily operations and overall strategy.
16 Indeed, observers have commented on Defendant’s engineering-centric culture, and have
17 remarked that Defendant is run by its engineers.

18 44. Defendant’s mission, and the means that Defendant has used to accomplish it
19 through its various services and products, including Gmail, Google Docs, Buzz, and Google
20 Street View, have raised serious privacy concerns.

21 **B. Privacy Concerns Over Defendants’ Practices**

22 45. On March 17, 2009, EPIC asked the federal government to investigate Defendant’s
23 so-called cloud computing services, including Gmail and Google Docs. EPIC sought assessment
24 of the privacy and security safeguards used by Defendant’s online applications and a
25 determination whether the company had properly represented these safeguards. EPIC’s petition
26 arose, in part, from Defendant’s inadvertent sharing of certain Google Docs files with users
27 unauthorized to view them, despite Defendant’s representations on its homepage that its services
28 were private and secure.

1 46. In February 2010, Defendant unveiled Buzz, a social networking service featuring
2 a Gmail add-on that automatically exposed users' most frequent email and chat contacts to the
3 general public. Soon thereafter, EPIC alleged that the service violated user expectations,
4 diminished user privacy, and contradicted Defendant's privacy policy. EPIC also noted that Buzz
5 may have violated federal wiretap laws. Defendant has recently announced that, as part of a
6 class action settlement, it will change its policies regarding Google Buzz to address users' privacy
7 concerns.

8 47. Absent a lawsuit, concerns about privacy appear to have fallen on deaf ears.
9 Google seems to believe that its quest to organize and make accessible the world's data is vastly
10 more important than concerns about individual privacy. Google also seems to believe that the
11 ability opt out of its grand ambition cures any individual issues there may be. With regard to the
12 Company's massive Street View project, Google CEO Eric Schmidt has said publicly that those
13 people concerned that photographs of their homes can be easily accessed around the world via the
14 internet should "just move," *see* Wall St. J. October 26, 2010, and that "Google's policy was to
15 'get right up to the creepy line,' but not cross it."

16 [http://www.huffingtonpost.com/2010/10/25/google-ceo-suggests-you-](http://www.huffingtonpost.com/2010/10/25/google-ceo-suggests-you-m_n_773388.html?ref=email_share)
17 [m_n_773388.html?ref=email_share](http://www.huffingtonpost.com/2010/10/25/google-ceo-suggests-you-m_n_773388.html?ref=email_share). Schmidt has also been dismissive of privacy concerns,
18 stating in a December 2009 CNBC interview that "[i]f you have something that you don't want
19 anyone to know, maybe you shouldn't be doing it in the first place."

20 48. Defendants' disregard for privacy has caught the attention of governmental
21 agencies and politicians across the globe. Australian communications minister Conroy said of
22 Defendant's track record on privacy in the May 26, 2010 edition of *The Australian*: "This is a
23 company that says 'do no evil' but tries to pretend it is not motivated by profit and that it knows
24 best and 'you can trust us' when it comes to privacy. Unfortunately there are no safeguards.
25 They consider themselves to be above government."

26 49. Privacy authorities from 10 countries—including Canada, France, Germany,
27 Ireland, Israel, Italy, the Netherlands, New Zealand, Spain, and the United Kingdom—issued a
28 forcefully worded letter to Defendant on April 19, 2010 about its privacy practices in general and

1 regarding Google Buzz and Google Street View in particular. The group said that Defendant too
2 often had “failed to take adequate account of privacy considerations when launching new
3 services,” and that it needed to build privacy safeguards and controls directly into new products
4 as they were being designed, rather than trying to apply them later. Among the minimum
5 suggested safeguards urged was “collecting and processing only the minimum amount of personal
6 information necessary to achieve the identified purpose of the product or service.”

7 50. Defendant’s conduct also has caught the attention of numerous privacy
8 organizations, which have given Defendant abysmal marks.

9 51. Public Information Research, Inc. (“PIR”), a non-profit organization, “specializes
10 in monitoring privacy violations on the web.” In 2002, PIR launched a website called Google
11 Watch, which advertised itself as “a look at Google’s monopoly, algorithms, and privacy issues.”
12 The site questioned Google’s storage of cookies, which in 2007 had a life span exceeding
13 32 years and incorporated a unique ID that enabled the creation of a user data log. In February
14 2003, Google Watch nominated Defendant for a “Big Brother Award,” calling Defendant a
15 “privacy time bomb.”

16 52. Privacy International (“PI”), a non-profit organization based in London with
17 offices in Washington, D.C., is the world’s oldest surviving privacy advocacy group in the world.
18 In its 2007 Consultation Report, PI ranked Defendant as “Hostile to Privacy,” the lowest ranking
19 available. Defendant was the only company on the list to receive that ranking. PI noted
20 Defendant’s “[t]rack history of ignoring privacy concerns. Every corporate announcement
21 involves some new practice involving surveillance. Privacy officer tries to reach out but no
22 indication that this has any effect on product and service design or delivery.” PI further noted, in
23 a section titled “Openness and Transparency,” Defendant’s “[v]ague, incomplete and possibly
24 deceptive privacy policy.” And in a section titled “Ethical Compass,” PI commented that
25 Defendant’s “[p]rivacy mandate is not embedded throughout the company. Techniques and
26 technologies frequently rolled out without adequate public consultation (*e.g.*, Street level view).”
27
28

1 **C. Google Street View**

2 53. Defendant's historically nonchalant attitude towards privacy concerns has carried
3 through, unfortunately, to its development and implementation of Google Street View.

4 54. Google Street View is a technology featured in Defendant's Google Maps and
5 Google Earth products that offers panoramic views from various positions along many streets
6 across the globe.

7 55. Defendant first launched Google Street View on May 25, 2007 in several select
8 cities across the United States. Since that time, Google Street View has expanded to include
9 more cities and rural areas across the United States and worldwide, and Google Street View now
10 is offered in more than 30 countries. Google Street View displays images taken from a fleet of
11 specially adapted cars known as Google Street View vehicles. On the top of each Street View
12 vehicle, Google placed nine directional cameras to capture 360 degree views. Google also
13 equipped the vehicles with 3G/GSM/Wi-Fi antennas and sophisticated, custom-designed
14 hardware and software for the capture and storage of wireless signals and data.

15 56. On May 29, 2007, Google issued a press release titled "Google Announces New
16 Mapping Innovations at Where 2.0 Conference." In discussing its new project, Google described
17 how it would allow users to view 360 degree street level imagery, but Google did not disclose
18 that it also intended to intercept electronic communications and illegally obtain private data.

19 57. Pictures of Google Street View vehicles on display and in action follow:





1
2
3
4
5
6
7
8
9
10
11 58. For areas inaccessible by automobile, like pedestrian walkways, narrow streets,
12 alleys, parks and ski resorts, Defendant has turned to smaller vehicles, such as Google Trikes
13 (tricycles) or snowmobiles, to provide coverage. The same directional cameras and antennae
14 placed on top of Google Street View vehicles also are placed on Google Trikes.

15 59. On October 16, 2009, Google issued a press release discussing its Google Trikes
16 and described them as “specially decorated unit[s] with imaging and GPS technology.” Google
17 never disclosed to the public that the trikes were also designed to and did in fact collect payload
18 data such as personal email and passwords.

19 60. Before Google Street View vehicles first hit the streets in mid-2007, Defendant
20 spent several months hard at work developing a sophisticated data collection system that would
21 be utilized by each vehicle to collect WiFi data.

22 61. In 2006, Defendant’s engineers intentionally created a data collection system to
23 include code that sampled and collected, decoded and analyzed all types of data broadcast
24 through WiFi connections. This type of system is known among experts as a packet analyzer,
25 wireless sniffer, network analyzer, packet sniffer, or protocol analyzer.

26 62. As data streams flow across the WiFi connections, a wireless sniffer secretly
27 captures each packet of information, then decodes or decrypts and analyzes its contents according
28 to the appropriate specifications.

1 63. To view data secretly captured by a wireless sniffer in readable form, it must be
2 stored on digital media and then decoded using crypto-analysis or similar complicated
3 technology.

4 64. The data, as initially captured by the wireless sniffer, are not readable by members
5 of the public absent sophisticated decoding and processing technology.

6 65. The data collection hardware and software technology that Google developed was
7 approved by Defendant before authorizing its inclusion in the Google Street View vehicles and
8 sending them off into the world to obtain information. In fact, Google sought to patent the
9 process.

10 66. The data that the Google Street View vehicles intercepted and collected included
11 Class members' SSID information, MAC address, usernames, passwords, and personal emails—
12 note of which Defendant needed for Google Street View and the interception of which was not
13 disclosed until months or years later.

14 67. Defendant did not publicly disclose, until the spring of 2010, that it had been using
15 Google Street View vehicles to intercept and collect WiFi data, as opposed to simply collecting
16 Street View images to post on its Google Maps and Google Earth services. Prior to that time,
17 Google concealed the scope of its data gathering. For example, on October 7, 2009, Google
18 issued a press release discussing its Street View application in Canada and directly
19 misrepresented the truth about the data it was collecting. Rather than admit that it had created
20 software that was used to collect personal payload data, it said, "Google has gone to great lengths
21 to ensure Canadians' privacy while enabling them to benefit from Street View on Google Maps.
22 The feature only contains imagery that is already visible from public roads and blurs identifiable
23 faces and license plates. In addition, users can easily flag for removal images that they consider
24 sensitive or inappropriate by clicking on the "Report a problem" link at the bottom of any image.

25 68. Google misrepresented the nature of its Street View program by concealing the
26 fact that it was doing more than just collecting and displaying images that were publicly
27 available. Google's surreptitious data collection also violated its own well-publicized privacy
28 policy. Google's longstanding privacy policy has for years stated that "we will not collect or use

1 sensitive information for purposes other than those described in this Privacy Policy and/or in the
2 supplementary service privacy notices, *unless we have obtained your prior consent.*” (Emphasis
3 added.) Tellingly, Google deleted this portion of the policy in an October 2010 revision of the
4 policy after its surreptitious data gathering through its Street View program was exposed.

5 **D. Defendant’s Admissions Regarding Interception Of Payload Data**

6 69. On April 27, 2010, Google posted an entry on its European Public Policy Blog in
7 response to inquiries from the German Data Protection Authority (“DPA”) concerning the
8 specific data Google Street View vehicles collected. In this post, Google explained that it
9 collected the SSID (the Wi-Fi network name) and MAC address (basically the ID number of the
10 Wi-Fi network’s hardware). [http://googlepolicyeuropa.blogspot.com/2010/04/data-collected-by-](http://googlepolicyeuropa.blogspot.com/2010/04/data-collected-by-google-cars.html)
11 [google-cars.html](http://googlepolicyeuropa.blogspot.com/2010/04/data-collected-by-google-cars.html).

12 70. In this April 27 post, however, Google claimed it did not collect any payload data.
13 *See id.* That statement turned out to be false.

14 71. In May 2010, after the DPA asked to audit the WiFi data collected by the Google
15 Street View vehicles, Defendant admitted in a blog post that the information in its April 27 post
16 was wrong, and that it indeed had been “collecting samples of payload data from open (i.e. non-
17 password-protected) WiFi networks.”

18 72. In fact, Defendant admitted that “[i]n 2006, an engineer working on an
19 experimental WiFi project wrote a piece of code that sampled all categories of publicly broadcast
20 WiFi data,” which was eventually used to collect and store the payload data. *Id.*

21 73. Defendant also admitted that “it has accumulated about 600 gigabytes of data
22 transmitted over public Wi-Fi networks in more than 30 countries.” [http://news.cnet.com/8301-](http://news.cnet.com/8301-30686_3-20005051-266.html)
23 [30686_3-20005051-266.html](http://news.cnet.com/8301-30686_3-20005051-266.html).

24 74. Defendant’s admissions, however, do not go far enough. Defendant should also
25 have admitted that the payload data it collected had not been publicly broadcast

26 75. Defendant further admitted that it had collected and stored “snippets of e-mails
27 and other internet activity within those homes.” [http://www.ft.com/cms/s/2/8a23b394-5fab-11df-](http://www.ft.com/cms/s/2/8a23b394-5fab-11df-a670-00144feab49a.html?ftcamp=rss)
28 [a670 00144feab49a.html?ftcamp=rss](http://www.ft.com/cms/s/2/8a23b394-5fab-11df-a670-00144feab49a.html?ftcamp=rss). Eric Schmidt, Defendant’s chief executive, “admitted that

1 he could not rule out the possibility that personal data such as bank account details were among
2 the data collected.” He admitted that ““We screwed up. Let’s be clear about that.””

3 <http://www.ft.com/cms/s/2/db664044-6f43-11df-9f43-00144feabdc0.html>. Likewise, Google co-
4 founder Sergey Brin admitted that Google’s actions were wrong. Speaking at the Google I/O
5 conference on May 19, 2010, Brin said: ““In short, let me just say that we screwed up. I’m not
6 going to make any excuses about it. The answer is yes. We do have a lot of internal controls in
7 place but obviously they didn’t prevent this error from occurring.””

8 [http://www.zdnet.com/blog/btl/sergey-brin-we-screwed-up-on-wifi-data-
9 collection/34759?tag=content;search-results-rivers](http://www.zdnet.com/blog/btl/sergey-brin-we-screwed-up-on-wifi-data-collection/34759?tag=content;search-results-rivers).

10 76. Notwithstanding these stunning admissions, Google took pains to claim that
11 whatever it had collected was likely fragmentary. This explanation turned out to be misleading,
12 at best.

13 77. In October 2010, Google was forced to admit in the face of continuing
14 investigations that their collection efforts had captured whole emails, usernames, passwords, and
15 other private data that individuals were using within the privacy of their own homes. Defendant’s
16 Senior VP of Engineering & Research, Alan Eustace, stated that “a number of external regulators
17 have inspected data as part of their investigations It’s clear from those inspections that while
18 most of the data is fragmentary, in some instances entire emails and URLs were captured, as well
19 as passwords. We want to delete this data as soon as possible, and I would like to apologize again
20 for the fact that we collected it in the first place.”

21 <http://googleblog.blogspot.com/2010/10/creating-stronger-privacy-controls.html>.

22 **E. Governmental Investigations In The United States**

23 78. Since the exposure of Defendant’s illicit activities by the German DPA, several
24 governmental entities in the United States have commenced their own investigations into
25 Defendant’s Google Street View conduct.

26 79. House Energy and Commerce ranking member Joe Barton, R-Texas, senior
27 committee member Edward Markey, D-Massachusetts, and chairman Henry Waxman, D-
28 California, commenced their own investigation into Defendant’s Street View conduct. They sent

1 a letter to Eric Schmidt of Google on May 26, 2010, asking Defendant to respond to various
2 inquiries and expressing concern that:

3 Google gathered more than 600 gigabytes of data from Wi-Fi
4 networks in more than 30 countries. Presumably this data could
5 include personal emails, health and financial information, and
6 search and surfing habits.

7 ***

8 In particular, we are concerned that Google did not disclose until
9 long after the fact that consumers' Internet use was being recorded,
10 analyzed and perhaps profiled. In addition, we are concerned about
11 the completeness and accuracy of Google's public explanations
12 about this matter.

13 *See* May 26, 2010 Letter to Eric Schmidt from Representatives Barton, Markey and Waxman.

14 80. Defendant responded on June 9, 2010 confirming that it "included code in [its]
15 software that collected samples of 'payload data'" and that "[i]t is possible that the payload data
16 may have included personal data if a user at the moment of collection broadcast such
17 information..." Defendant also stated that it had been "collecting WiFi data via Street View cars
18 in the United States" since 2007. *See* June 9, 2010 Letter to Chairman Waxman, and
19 Representatives Barton and Markey from Pablo Chavez, Defendant's Director of Public Policy.

20 81. Connecticut Attorney General, Richard Blumenthal, has also commenced a
21 multistate investigation, on behalf of a 38 states, into Defendant's "Google Street View cars"
22 unauthorized collection of personal data from wireless computer networks."

23 <http://www.ct.gov/ag/cwp/view.asp?Q=461862&A=3869>.

24 82. The coalition includes such states as Texas, Florida, Kentucky, Illinois, Missouri,
25 and Massachusetts. <http://latimesblogs.latimes.com/technology/2010/07/google-street-view.html>.

26 **F. Foreign Governmental Investigations**

27 83. Defendants' admissions also caused numerous foreign governments to take note,
28 with several foreign governmental agencies and authorities already having initiated investigations
29 into Defendant's conduct.

30 84. According to the Associated Press, on May 15, 2010, Germany's minister of
31 consumer protection, Ilse Aigner, referred to Defendant's conduct as "alarming," and remarked

1 that “[a]ccording to the information available to us so far, [Defendant] has for years penetrated
2 private networks, apparently illegally.”

3 http://voices.washingtonpost.com/posttech/2010/05/german_official_rebukes_google.html.

4 85. On May 19, 2010, German prosecutors based in Hamburg announced the opening
5 of a criminal investigation into Defendant’s conduct, according to *The New York Times*.

6 86. After repeated requests by German data protection officials, in September 2010,
7 Defendant finally gave the officials “a full copy of the Internet and e-mail data it said it
8 inadvertently collected from Wi-Fi routers while compiling its Street View archive.”

9 <http://www.nytimes.com/2010/10/16/technology/16streetview.html>.

10 87. According to Johannes Casper, the data protection supervisor in Hamburg, “We
11 have the hard drives now from Google, ... [b]ut the data is so massive and diverse that we are
12 having to develop our own software programs to analyze what was collected and how. This will
13 take a bit of time.” *Id.*

14 88. The Italian data protection agency announced on May 19, 2010 that it was seeking
15 information on when Defendant began collecting the data, the reason for doing so, the length of
16 time for which it has been doing so, where the data were stored, and whether it has been sold.
17 That agency also is inquiring whether Defendant shared the data with third parties.

18 <http://www.networkworld.com/news/2010/051910-google-street-view-faces-investigation.html>.

19 89. Most recently, the Italian data protection agency issued a press release on
20 September 21, 2010, stating that Defendant had confirmed “that payload data had actually been
21 captured by its cars.” <http://www.garanteprivacy.it/garante/doc.jsp?ID=1751001>.

22 90. In fact, Defendant stated in a June 1, 2010 letter to the Italian data protection
23 agency that “that had been collecting payload data since April 2008 when the StreetView cars
24 were driving through Italy, using Wi-Fi antenna and ad-hoc software for this purpose.”

25 <http://www.garanteprivacy.it/garante/doc.jsp?ID=1750713>.

26 91. On May 19, 2010, the Spanish data protection agency also ordered the
27 commencement of an investigation into whether Defendant violated laws governing personal
28 data. http://www.theregister.co.uk/2010/06/14/street_view_spain/.

1 92. The Spanish data protection agency has recently announced that its investigation
2 has led it to file suit against Defendant, as it has “evidence of five offences committed by Google
3 involving the capturing and storing of data from users connected to Wi-Fi networks while
4 collect[ing] photographs for Street View and the transfer of such data to the United States.”
5 http://news.yahoo.com/s/afp/20101018/tc_afp/spaininternetitcourtrightsgoogle.

6 93. Furthermore, Spain’s Association for the Prevention and Investigation of Crime,
7 Abuse and Malpractice in Information Technology and Advanced Communication
8 (“Apedancia”), filed a lawsuit against Defendant in the Police Court of Madrid. Regarding
9 Defendant’s assertion that its interception and collection of the WiFi payload data was a mistake,
10 Apedancia president Miguel Angel Callardo stated that ““something which was carefully
11 programmed and has been done in 30 countries can’t be an error.””
12 http://www.theregister.co.uk/2010/06/14/street_view_spain/.

13 94. In May 2010, the French National Commission on Computing and Liberty
14 (“CNIL”) reported that it would begin investigating Defendant. Noting Defendant’s admission
15 that it had collected Wi-Fi data traffic, the CNIL said, ““This collection was not mentioned in
16 Google’s declaration to the CNIL. That’s why the Commission is currently conducting a review
17 of Google, in order to obtain all the information on this case and decide what action to take.””
18 <http://www.networkworld.com/news/2010/051910-google-street-view-faces-investigation.html>.

19 95. On June 17, 2010, the CNIL issued a press release stating that Defendant, through
20 its interception and collection of the Wi-Fi payload data, gained access to passwords for email
21 accounts, as well as excerpts of electronic messages. <http://www.bbc.co.uk/news/10364073>.

22 96. CNIL chairman Alex Turk said that data which Defendant had handed over to the
23 CNIL preliminarily “showed the presence of ‘data that are normally covered by banking . . . and
24 medical privacy rules.’” *Id.*

25 97. The Czech Office for Personal Data Protection has been looking into potential
26 issues with Google Street View since April 2010. [http://www.praguepost.com/business/4531-
27 google-under-investigation-for-stealing-private-data.html](http://www.praguepost.com/business/4531-google-under-investigation-for-stealing-private-data.html).

1 98. Most recently, the Czech Republic has banned Defendant's Street View cars
2 pending its investigation into the legality of Defendant's activities.

3 [http://news.softpedia.com/news/Czechs-Ban-Google-Street-View-Cars-Pending-Investigation-
4 156569.shtml](http://news.softpedia.com/news/Czechs-Ban-Google-Street-View-Cars-Pending-Investigation-156569.shtml).

5 99. On July 9, 2010, Australian Privacy Commissioner Karen Curtis concluded her
6 investigation into defendant's Street View activities and stated that "[o]n the information
7 available I am satisfied that any collection of personal information would have breached the
8 Australian Privacy Act." She further stated that "[c]ollecting personal information in these
9 circumstances is a very serious matter. Australians should reasonably expect that private
10 communications remain private." <http://www.privacy.gov.au/materials/a-z?fullsummary=7103>.

11 100. Defendant, on that same day, issued an apology on its Official Google Australia
12 Blog, entitled "We're sorry." It stated, in pertinent part, that:

13 A couple of years ago, Google started collecting WiFi network
14 information via our Street View cars to improve location-based
15 services like search and maps. In May, we announced that we had
16 also mistakenly been collecting publicly broadcast payload data
17 (information sent over the network). . . . We want to reiterate to
Australians that this was a mistake for which we are sincerely sorry.
Maintaining people's trust is crucial to everything we do and we
have to earn that trust every single day. We are acutely aware that
we failed badly here.

18 <http://google-au.blogspot.com/2010/07/were-sorry.html>. Google's apology, however, should also
19 have acknowledged that the payload data it had collected had not been publicly broadcast.

20 101. Stephen Conroy, Australia's minister for broadband, communications and the
21 digital economy, later stated that Defendant's secret data interceptions constitute the "single
22 greatest breach in the history of privacy."

23 <http://www.guardian.co.uk/technology/2010/oct/19/google-street-view-privacy-canada>.

24 102. Likewise, in Canada, it has been determined that Defendant's "Street View feature
25 violated Canada's privacy law by accessing personal information from unsecured wireless
26 networks." Furthermore, Canada's privacy office said that "[t]housands of Canadians may have
27 given up information such as usernames, passwords and a list of contact information for people
28

1 with medical conditions.” [http://www.bloomberg.com/news/2010-10-19/canada-privacy-](http://www.bloomberg.com/news/2010-10-19/canada-privacy-commissioner-says-google-broke-privacy-laws-with-networks.html)
2 [commissioner-says-google-broke-privacy-laws-with-networks.html](http://www.bloomberg.com/news/2010-10-19/canada-privacy-commissioner-says-google-broke-privacy-laws-with-networks.html).

3 103. Furthermore, Jennifer Stoddart, the Canadian privacy commissioner, stated that
4 “[o]ur investigation shows that Google did capture personal information—and, in some cases,
5 highly sensitive personal information such as complete e-mail addresses, usernames and
6 passwords.” [http://www.guardian.co.uk/technology/2010/oct/19/google-street-view-privacy-](http://www.guardian.co.uk/technology/2010/oct/19/google-street-view-privacy-canada)
7 [canada](http://www.guardian.co.uk/technology/2010/oct/19/google-street-view-privacy-canada).

8 104. In June 2010, the Hungarian Parliamentary Commissioner for Data Protection and
9 Freedom of Information announced its investigation into Google Street View. That same month,
10 the Privacy Commissioner, Jóri András, sent a letter to Defendant containing several inquiries
11 into Defendant’s interception and collection of Wi-Fi payload data contained on private networks.
12 http://abiweb.obh.hu/abi/index.php?menu=0/Sajtokozlemenyek&dok=20100604_ABI_2;
13 http://abiweb.obh.hu/dpc/index.php?menu=aktualis/allasfoglalasok/2010&dok=20090602_ABI_1

14 .
15 105. After learning of the privacy concerns with Google Street View, Ireland’s Data
16 Protection Authority requested that Defendant delete the data it obtained from Irish networks.
17 Defendant eventually complied.
18 http://voices.washingtonpost.com/posttech/2010/05/google_said_monday_afternoon_t.html.

19 106. In June 2010, the Korea Communications Commission began an investigation into
20 Google Street View after Defendant revealed that it intercepted and collected “parts of personal
21 information while preparing to service its Street View program” in Korea.
22 <http://www.koreaherald.com/business/Detail.jsp?newsMLId=20100608000599>.

23 107. In August 2010, the Korean National Police Agency stated that “[The police]
24 have been investigating Google Korea LLC on suspicion of unauthorized collection and storage
25 of data on unspecified Internet users from Wi-Fi networks.”
26 [http://www.dailytech.com/Google+Street+View+Under+Investigation+in+South+Korea/article19](http://www.dailytech.com/Google+Street+View+Under+Investigation+in+South+Korea/article19305.htm)
27 [305.htm](http://www.dailytech.com/Google+Street+View+Under+Investigation+in+South+Korea/article19305.htm).

1 108. Also in August 2010, police in South Korea raided Defendant's Seoul office and
2 confiscated materials as part of its investigation into the privacy concerns of Defendant's activity.
3 [http://www.bloomberg.com/news/print/2010-08-10/google-s-south-korea-office-raided-by-police-](http://www.bloomberg.com/news/print/2010-08-10/google-s-south-korea-office-raided-by-police-in-invasion-of-privacy-probe.html)
4 [in-invasion-of-privacy-probe.html](http://www.bloomberg.com/news/print/2010-08-10/google-s-south-korea-office-raided-by-police-in-invasion-of-privacy-probe.html).

5 109. On May 14, 2010, New Zealand Privacy Commissioner Marie Shroff announced
6 the commencement of an investigation into Defendant's Google Street View activity and said that
7 "I am surprised that the public was not more clearly told beforehand if Google would be
8 collecting other information with its Street View cars." [http://www.privacy.org.nz/media-](http://www.privacy.org.nz/media-release-google-and-wi-fi-information-collection/)
9 [release-google-and-wi-fi-information-collection/](http://www.privacy.org.nz/media-release-google-and-wi-fi-information-collection/).

10 **V. TOLLING AND FRAUDULENT CONCEALMENT**

11 110. Plaintiffs and members of the Class did not discover, and could not have
12 discovered through the exercise of reasonable diligence, the existence of Defendant's conduct
13 alleged herein until May 14, 2010, when Defendant first admitted that it had been collecting and
14 storing the Class members' WiFi data, including payload data, via Google Street View.

15 111. Because Defendant kept its conduct secret until May 14, 2010, Plaintiffs and
16 members of the Class before that time were unaware of Defendant's unlawful conduct alleged
17 herein.

18 112. The acts of Defendant alleged herein were wrongfully concealed and carried out in
19 a manner that precluded detection.

20 113. By its very nature, Defendant's conduct was inherently self-concealing.

21 114. A reasonable person under the circumstances would not have been alerted to
22 investigate Defendant's conduct alleged herein until at least May 14, 2010.

23 115. Plaintiffs and members of the Class could not have discovered Defendant's
24 conduct at an earlier date by the exercise of reasonable diligence because of the deceptive
25 practices and sophisticated technology employed by Defendant to avoid detection.

26 116. None of the facts or information available to Plaintiffs and members of the Class
27 prior to May 14, 2010, if investigated with reasonable diligence, could or would have led to the
28 discovery of Defendant's conduct alleged herein prior to that date.

1 117. As a result of Defendant's fraudulent concealment, the running of any statute of
 2 limitations has been tolled with respect to the claims that Plaintiffs and members of the Class
 3 have alleged in this Complaint.

4 118. In addition, the claims of Plaintiffs and the Class members did not accrue until
 5 they knew of Defendant's unlawful conduct and corresponding legal violations.

6 **VI. CLASS ACTION ALLEGATION**

7 119. Plaintiffs bring this action on behalf of themselves and as a class action under
 8 Rule 3(a) and (b)(1)(2) and (3) of the Federal Rules of Civil Procedure on behalf of the following
 9 class (the "Class"):

10 • **National Class (Wiretapping and Unfair Competition):**

11 All persons in the United States whose electronic
 12 communications sent or received on wireless internet
 13 connections were intercepted by Defendant's Google Street
 14 View vehicles from May 25, 2007 through the present.
 Excluded from the Class are Defendant, including
 subsidiaries and affiliates, federal governmental entities and
 instrumentalities, and the court and court personnel.

15 • **State Subclasses (Wiretapping):**

16 All persons in the each of the following states whose
 17 electronic communications sent or received on wireless
 18 internet connections were intercepted by Defendant's
 19 Google Street View vehicles from May 25, 2007 through
 20 the present: Arizona, Hawaii, Minnesota, Nebraska, Ohio,
 21 South Carolina, Utah, Tennessee, Missouri, Washington,
 Pennsylvania, Nevada and Texas. Excluded from these
 Subclasses are Defendant, including subsidiaries and
 affiliates, federal governmental entities and
 instrumentalities, and the court and court personnel.

22 120. Plaintiffs believe that there are tens of thousands, and perhaps millions, of
 23 National Class members located throughout the United States, the exact number and their
 24 identities being knowable by Defendant, making the National Class so numerous and
 25 geographically dispersed that joinder of all members is impracticable.

26 121. Similarly, Plaintiffs believe that there are thousands of State Subclass members in
 27 each of the listed states.
 28

1 122. There are questions of law and fact common to the National Class and the State
2 Subclasses, including:

3 a. Whether Defendant intentionally intercepted National Class members'
4 electronic communications sent or received on WiFi connections, in violation of 18 U.S.C.
5 § 2511, *et seq.*;

6 b. The appropriate amount of statutory damages that should be awarded to the
7 National Class under 18 U.S.C. § 2520;

8 c. The appropriate amount of punitive damages that should be awarded to the
9 National Class under 18 U.S.C. § 2520;

10 d. Whether the National Class is entitled to, and the appropriate types of,
11 equitable or declaratory relief under 18 U.S.C. § 2520;

12 e. Whether Defendant intentionally intercepted Sub-class members'
13 electronic communications sent or received on WiFi connections, in violation of state wiretap
14 statutes in Arizona, Hawaii, Minnesota, Nebraska, Ohio, South Carolina, Utah, Tennessee,
15 Missouri, Washington, Pennsylvania, Nevada and Texas which are substantially similar to
16 18 U.S.C. § 2511, *et seq.*;

17 f. The appropriate amount of statutory damages that should be awarded to the
18 Sub-class under state wiretap statutes in Arizona, Hawaii, Minnesota, Nebraska, Ohio, South
19 Carolina, Utah, Tennessee, Missouri, Washington, Pennsylvania, Nevada and Texas which are
20 substantially similar to 18 U.S.C. § 2511, *et seq.*;

21 g. The appropriate amount of punitive damages that should be awarded to the
22 Sub-class under state wiretap statutes in Arizona, Hawaii, Minnesota, Nebraska, Ohio, South
23 Carolina, Utah, Tennessee, Missouri, Washington, Pennsylvania, Nevada and Texas which are
24 substantially similar to 18 U.S.C. § 2511, *et seq.*; and

25 h. Whether the Sub-class is entitled to, and the appropriate types of, equitable
26 or declaratory relief under state wiretap statutes in Arizona, Hawaii, Minnesota, Nebraska, Ohio,
27 South Carolina, Utah, Tennessee, Missouri, Washington, Pennsylvania, Nevada and Texas which
28 are substantially similar to 18 U.S.C. § 2511, *et seq.*

1 129. Beginning at least as early as May 25, 2007, Google intentionally intercepted, or
2 procured another person to intercept electronic communications of members of the National Class
3 in violation of 18 U.S.C. § 2511, *et seq.* (the “Federal Wiretap Statute”).

4 130. The electronic communications Google intercepted or procured another person to
5 intercept were intercepted from networks that were not configured so that such communications
6 were readily accessible to the general public.

7 131. The software, hardware, code, devices and/or processes Google has created,
8 configured, and employed in its Street View program are complex and not available to the general
9 public.

10 132. Pursuant to 18 U.S.C. § 2520, Plaintiffs and National Class members are each
11 entitled to the following:

- 12 • Statutory damages of whichever is the greater of \$100 a day
13 for each day of violation or \$10,000 per class member;
- 14 • Punitive damages in an amount to be determined by the
15 jury;
- 16 • Equitable, declaratory and/or injunctive relief as is deemed
17 appropriate; and
- 18 • Reasonable attorneys’ fees and other costs.

19 **SECOND CLAIM FOR RELIEF**
20 **Violation Of California Business And Professional Code § 17200, *et seq.***

21 133. Plaintiffs incorporate the previous paragraphs of this Complaint as if fully set forth
22 herein.

23 134. The conduct of Google, headquartered in California, set forth in the paragraphs
24 above, constitutes one or more acts of unfair competition within the meaning of California
25 Business and Professional Code § 17200, *et seq.*

26 135. Upon information and belief, many of the illegal acts complained of herein
27 emanated from, were supervised, coordinated and/or approved by Google personnel in California.
28 The hardware, software and business method used by Google for its illegal acts was developed,
tested and used in California.

1 143. The software, hardware, code, devices and/or processes Google employs in its
2 Street View program are complex and not available to the general public.

3 144. The State Wiretap Statutes provide a remedy in addition to the Federal Wiretap
4 Statute and is not pre-empted by the Federal Wiretap Statute.

5 145. In addition to relief and damages under the Federal Wiretap Statute, State Subclass
6 members are also each entitled to the following awards and relief:

- 7 • Statutory damages;
- 8 • Punitive damages in an amount to be determined by the
9 jury;
- 10 • Equitable, declaratory or injunctive relief as is deemed
appropriate; and
- 11 • Reasonable attorneys' fees and costs.

12 **VII. DEMAND FOR JURY TRIAL**

13 Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiffs demand a jury
14 trial as to all issues triable by a jury.

15 **VIII. PRAAYER FOR RELIEF**

16 WHEREFORE, Plaintiffs pray as follows:

17 A. That the Court determine that this action may be maintained as a class action under
18 Rule 23(a) and (b)(1), (2) and (3) of the Federal Rules of Civil Procedure.

19 B. That Defendant's conduct be adjudged to have violated 18 U.S.C. § 2511, *et seq.*,

20 C. That Defendant's conduct be adjudged to have violated the wiretap statutes of
21 Arizona (A.R.S. § 12-731), Hawaii (HRS § 803-41, *et seq.*), Minnesota (M.S.A. § 626A.01, *et*
22 *seq.*), Nebraska (Neb. Rev. St. § 86-271, *et seq.*), Ohio (R.C. § 2933.51, *et seq.*), South Carolina
23 (SC ST § 17-30-10, *et seq.*), Utah (U.C.A. 1953 § 77-23a-1, *et seq.*), Tennessee (T.C.A. 39-13-
24 601, *et seq.*), Missouri (MO ST 542.400, *et seq.*), Washington (WA ST 9.73.010, *et seq.*),
25 Pennsylvania (PA ST 18 Pa C.S.A. § 5703, *et seq.*), Nevada (N.R.S. § 200.610, *et seq.*) and
26 Texas (Tex. Civ. Prac. & Rem. § 123.001, *et seq.*) that are substantially similar to 18 U.S.C.
27 § 2511, *et seq.*

28 D. Injunctive and declaratory relief pursuant to California Business and Professional

1 Code § 17200, *et seq.*, including but not limited to prohibiting Defendant from making use of or
2 disseminating any wireless data collected through its practices described in this Complaint;
3 enjoining Defendant from engaging in the alleged conduct; and mandating a time and manner for
4 the disposition of the communications captured and stored by Defendant;

5 E. That Defendant be ordered to disgorge profits and revenues derived from its
6 course of conduct in violation of California Business and Professional Code § 17200, and that
7 such unjust enrichment be restored to the class and or distributed *cy pres* as the Court shall deem
8 just and equitable;

9 F. That judgment be entered for Plaintiff and National Class members against
10 Defendant for statutory damages as provided in 18 U.S.C. § 2520;

11 G. That judgment be entered against Defendant for statutory damages as provided in
12 Arizona (A.R.S. § 12-731), Hawaii (HRS § 803-48.), Minnesota (M.S.A. § 626A.13), Nebraska
13 (Neb. Rev. St. § 86-297), Ohio (R.C. § 2933.65), South Carolina (SC ST § 17-30-135), Utah
14 (U.C.A. 1953 § 77-23a-11), Tennessee (T.C.A. 39-13-603), Missouri (MO ST 542.418),
15 Washington (WA ST 9.73.030), Pennsylvania (PA ST 18 Pa C.S.A. § 5725), Nevada (N.R.S.
16 § 200.690) and Texas (Tex. Civ. Prac. & Rem. § 123.004) that are substantially similar to
17 18 U.S.C. § 2511, *et seq.*

18 H.. That judgment be entered for Plaintiff and National Class members against
19 Defendant for punitive damages as appropriate as provided in 18 U.S.C. § 2520;

20 I. That judgment be entered against Defendant for punitive damages as appropriate
21 as provided in Arizona (A.R.S. § 12-731), Hawaii (HRS § 803-48.), Minnesota (M.S.A.
22 § 626A.13), Nebraska (Neb. Rev. St. § 86-297), Ohio (R.C. § 2933.65), South Carolina (SC ST
23 § 17-30-135), Utah (U.C.A. 1953 § 77-23a-11), Tennessee (T.C.A. 39-13-603), Missouri (MO ST
24 542.418), Washington (WA ST 9.73.030), Pennsylvania (PA ST 18 Pa C.S.A. § 5725), Nevada
25 (N.R.S. § 200.690) and Texas (Tex. Civ. Prac. & Rem. § 123.004) that are substantially similar to
26 18 U.S.C. § 2511, *et seq.*

27 J. That Plaintiffs and the National Class recover pre-judgment and post-judgment
28 interest as permitted by law.

1 K. That Plaintiffs and the National Class recover their costs of the suit, including
2 attorneys' fees, as provided by 18 U.S.C. § 2520, and as provided by Arizona (A.R.S. § 12-731),
3 Hawaii (HRS § 803-48.), Minnesota (M.S.A. § 626A.13), Nebraska (Neb. Rev. St. § 86-297),
4 Ohio (R.C. § 2933.65), South Carolina (SC ST § 17-30-135), Utah (U.C.A. 1953 § 77-23a-11),
5 Tennessee (T.C.A. 39-13-603), Missouri (MO ST 542.418), Washington (WA ST 9.73.030),
6 Pennsylvania (PA ST 18 Pa C.S.A. § 5725), Nevada (N.R.S. § 200.690) and Texas (Tex. Civ.
7 Prac. & Rem. § 123.004) that are substantially similar to 18 U.S.C. § 2511, *et seq.*

8 L. For such other and further relief as is just and proper under the circumstances.

9
10 Dated: November 8, 2010

COHEN MILSTEIN SELLERS & TOLL, PLLC

11 By: /s/ Daniel A. Small
12 Daniel A. Small

13 1100 New York Avenue, NW, Suite 500W
14 Washington, DC 20005
15 Tel. 202-408-4600
16 Fax. 202-408-4699

17 *Plaintiffs' Co-Lead Counsel*

18
19 Dated: November 8, 2010

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

20 By: /s/ Elizabeth J. Cabraser
21 Elizabeth J. Cabraser

22 275 Battery Street, 29th Floor
23 San Francisco, CA 94111-3339
24 Tel. 415-956-1000
25 Fax. 415-956-1008

26 *Plaintiffs' Liaison Counsel*
27
28