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

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

Plaintiff Co-Lead Counsel

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

Plaintiffs' Liaison Counsel

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE: GOOGLE, INC. STREET VIEW ELECTRONIC COMMUNICATIONS LITIGATION	No. 5:10-md-02184 JW **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

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

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

I. NATURE OF THE CASE

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

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

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

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

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

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

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

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

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

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

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

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

11. Most recently, U.K. authorities concluded that Google's actions violated U.K. data protection law. U.K. Information Commissioner Christopher Graham said Google's actions constituted a "significant breach" of data protection law. Mr. Graham added that his office would ask Google to sign a binding commitment to prevent future breaches and agree to an audit of its data protection practices in the U.K. http://online.wsj.com/article/SB10001424052748703506904575591963217799010.html?mod=WSJ_hp_MIDDLENexttoWhatsNewsForth.

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

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

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

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

II. JURISDICTION AND VENUE

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

16. Venue lies within this District under 28 U.S.C. § 1391(b)-(c) because: (a) Defendant conducts business in this District; (b) certain acts giving rise to the claims asserted in this Complaint occurred in this District; (c) the actions of Defendant alleged in this Complaint caused damage to certain of the Plaintiffs and a substantial number of Class members within this District; and (d) Defendant maintains an office in this District.

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

III. PARTIES

A. Plaintiffs

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B. Defendant

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

IV. FACTUAL ALLEGATIONS

A. Defendant's Business And Culture

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

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

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

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

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

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

B. Privacy Concerns Over Defendants' Practices

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

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

47. Absent a lawsuit, concerns about privacy appear to have fallen on deaf ears. Google seems to believe that its quest to organize and make accessible the world's data is vastly more important than concerns about individual privacy. Google also seems to believe that the ability opt out of its grand ambition cures any individual issues there may be. With regard to the Company's massive Street View project, Google CEO Eric Schmidt has said publicly that those people concerned that photographs of their homes can be easily accessed around the world via the internet should "just move," *see* Wall St. J. October 26, 2010, and that "Google's policy was to 'get right up to the creepy line,' but not cross it." 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, stating in a December 2009 CNBC interview that "[i]f you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."

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

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

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

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

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

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

C. Google Street View

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

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

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

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

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

58. For areas inaccessible by automobile, like pedestrian walkways, narrow streets, alleys, parks and ski resorts, Defendant has turned to smaller vehicles, such as Google Trikes (tricycyles) or snowmobiles, to provide coverage. The same directional cameras and antennae placed on top of Google Street View vehicles also are placed on Google Trikes.

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

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

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

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

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

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

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

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

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

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

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

D. Defendant's Admissions Regarding Interception Of Payload Data

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

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

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

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

73. Defendant also admitted that "it has accumulated about 600 gigabytes of data transmitted over public Wi-Fi networks in more than 30 countries." http://news.cnet.com/8301-30686_3-20005051-266.html.

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

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

he could not rule out the possibility that personal data such as bank account details were among the data collected." He admitted that "'We screwed up. Let's be clear about that.'" http://www.ft.com/cms/s/2/db664044-6f43-11df-9f43-00144feabdc0.html. Likewise, Google co-founder Sergey Brin admitted that Google's actions were wrong. Speaking at the Google I/O conference on May 19, 2010, Brin said: "'In short, let me just say that we screwed up. I'm not going to make any excuses about it. The answer is yes. We do have a lot of internal controls in place but obviously they didn't prevent this error from occurring.'" http://www.zdnet.com/blog/btl/sergey-brin-we-screwed-up-on-wifi-data-collection/34759?tag=content;search-results-rivers.

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

77. In October 2010, Google was forced to admit in the face of continuing investigations that their collection efforts had captured whole emails, usernames, passwords, and other private data that individuals were using within the privacy of their own homes. Defendant's Senior VP of Engineering & Research, Alan Eustace, stated that "a number of external regulators have inspected data as part of their investigations . . . . It's clear from those inspections that while most of the data is fragmentary, in some instances entire emails and URLs were captured, as well as passwords. We want to delete this data as soon as possible, and I would like to apologize again for the fact that we collected it in the first place." http://googleblog.blogspot.com/2010/10/creating-stronger-privacy-controls.html.

E. Governmental Investigations In The United States

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

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

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

> Google gathered more than 600 gigabytes of data from Wi-Fi networks in more than 30 countries. Presumably this data could include personal emails, health and financial information, and search and surfing habits.
>
> ***
>
> In particular, we are concerned that Google did not disclose until long after the fact that consumers' Internet use was being recorded, analyzed and perhaps profiled. In addition, we are concerned about the completeness and accuracy of Google's public explanations about this matter.

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

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

81. Connecticut Attorney General, Richard Blumenthal, has also commenced a multistate investigation, on behalf of a 38 states, into Defendant's "Google Street View cars' unauthorized collection of personal data from wireless computer networks." http://www.ct.gov/ag/cwp/view.asp?Q=461862&A=3869.

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

F. Foreign Governmental Investigations

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

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

that "[a]ccording to the information available to us so far, [Defendant] has for years penetrated private networks, apparently illegally." http://voices.washingtonpost.com/posttech/2010/05/german_official_rebukes_google.html.

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

86. After repeated requests by German data protection officials, in September 2010, Defendant finally gave the officials "a full copy of the Internet and e-mail data it said it inadvertently collected from Wi-Fi routers while compiling its Street View archive." http://www.nytimes.com/2010/10/16/technology/16streetview.html.

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

88. The Italian data protection agency announced on May 19, 2010 that it was seeking information on when Defendant began collecting the data, the reason for doing so, the length of time for which it has been doing so, where the data were stored, and whether it has been sold. That agency also is inquiring whether Defendant shared the data with third parties. http://www.networkworld.com/news/2010/051910-google-street-view-faces-investigation.html.

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

90. In fact, Defendant stated in a June 1, 2010 letter to the Italian data protection agency that "that had been collecting payload data since April 2008 when the StreetView cars were driving through Italy, using Wi-Fi antenna and ad-hoc software for this purpose." http://www.garanteprivacy.it/garante/doc.jsp?ID=1750713.

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

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

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

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

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

96. CNIL chairman Alex Turk said that data which Defendant had handed over to the CNIL preliminarily "showed the presence of 'data that are normally covered by banking . . . and medical privacy rules.'" *Id.*

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

98. Most recently, the Czech Republic has banned Defendant's Street View cars pending its investigation into the legality of Defendant's activities. http://news.softpedia.com/news/Czechs-Ban-Google-Street-View-Cars-Pending-Investigation-156569.shtml.

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

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

> A couple of years ago, Google started collecting WiFi network information via our Street View cars to improve location-based services like search and maps. In May, we announced that we had also mistakenly been collecting publicly broadcast payload data (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.

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

101. Stephen Conroy, Australia's minister for broadband, communications and the digital economy, later stated that Defendant's secret data interceptions constitute the "'single greatest breach in the history of privacy.'" http://www.guardian.co.uk/technology/2010/oct/19/google-street-view-privacy-canada.

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

with medical conditions." http://www.bloomberg.com/news/2010-10-19/canada-privacy-commissioner-says-google-broke-privacy-laws-with-networks.html.

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

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

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

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

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

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

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

V. TOLLING AND FRAUDULENT CONCEALMENT

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

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

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

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

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

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

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

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

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

VI. CLASS ACTION ALLEGATION

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

- **National Class (Wiretapping and Unfair Competition):**

  All persons in the United States whose electronic communications sent or received on wireless internet connections were intercepted by Defendant's Google Street 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.

- **State Subclasses (Wiretapping):**

  All persons in the each of the following states whose electronic communications sent or received on wireless internet connections were intercepted by Defendant's Google Street View vehicles from May 25, 2007 through the present: Arizona, Hawaii, Minnesota, Nebraska, Ohio, 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.

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

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

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

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

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

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

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

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

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

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

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

123. Plaintiffs' claims are typical of the claims of the members of the National Class and State Sub-classes, and Plaintiffs will fairly and adequately protect the interests of the National Class and State Sub-classes. Plaintiffs and all members of the National Class and State Sub-class are similarly affected by Defendant's wrongful conduct in violation of the federal wiretap statute in that their electronic communications transmitted over WiFi connections were intentionally intercepted by Defendant's Google Street View vehicles. Plaintiffs' claims arise out of the same common course of conduct giving rise to the claims of the other National Class and State Sub-class members. Plaintiffs' interests are coincident with, and not antagonistic to, those of the other National Class and State Sub-class members.

124. Plaintiffs are represented by counsel who are competent and experienced in the prosecution of class action litigation.

125. The prosecution of separate actions by individual members of the National Class and State Sub-classes would create a risk of inconsistent or varying adjudications, establishing incompatible standards of conduct for Defendant.

126. The questions of law and fact common to the members of the National Class and State Sub-classes predominate over any questions affecting only individual members.

127. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The National Class and State Sub-classes are readily definable. Prosecution as a class action will eliminate the possibility of repetitious litigation. Treatment as a class action will permit a large number of similarly situated persons to adjudicate their common claims in a single forum simultaneously, efficiently, and without the duplication of effort and expense that numerous individual actions would engender. This action presents no difficulties in management that would preclude maintenance as a class action.

FIRST CLAIM FOR RELIEF
National Class Claims – 18 U.S.C. § 2511, *et seq*.

128. Plaintiffs incorporate the previous paragraphs of this Complaint as if fully set forth herein.

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

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

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

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

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

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

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

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

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

136. The practices engaged in by Google are unfair because they are immoral, unethical, oppressive, unscrupulous and/or substantially injurious to the National Class members.

137. The practices engaged in by Google are unlawful because they violate the Federal Wiretap Statute and/or because they constitute invasion of class members' legally protected right to privacy under the California Constitution and other applicable law.

138. Plaintiffs and National Class members have suffered injury in fact and lost property as a result of the unfair and unlawful business practices.

139. Unless Google is enjoined from continuing to engage in, or resuming, these unfair and unlawful business practices and ordered to dispose of the wrongfully intercepted electronic communications, Plaintiffs and other National Class members will continue to be injured by the wrongful actions and conduct of Google.

THIRD CLAIM FOR RELIEF
(State Subclass Claims)

140. Plaintiffs incorporate the previous paragraphs of this Complaint as if fully set forth herein.

141. Beginning at least as early as May 25, 2007, Google intentionally intercepted, or procured any other person to intercept or electronic communications of members of the State Subclasses in violation of the state wiretap statutes in Arizona (A.R.S. § 12-731), Hawaii (HRS § 803-41, *et seq.*), Minnesota (M.S.A. § 626A.01, *et seq.*), Nebraska (Neb. Rev. St. § 86-271, *et seq.*), Ohio (R.C. § 2933.51, *et seq.*), South Carolina (SC ST § 17-30-10, *et seq.*), Utah (U.C.A. 1953 § 77-23a-1, *et seq.*), Tennessee (T.C.A. 39-13-601, *et seq.*), Missouri (MO ST 542.400, *et seq.*), Washington (WA ST 9.73.010, *et seq.*), Pennsylvania (PA ST 18 Pa C.S.A. § 5703, *et seq.*), Nevada (N.R.S. § 200.610, *et seq.*) and Texas (Tex. Civ. Prac. & Rem. § 123.001, *et seq.*) that are substantially similar to 18 U.S.C. § 2511, *et seq.*

142. The electronic communications Google intercepted or endeavored to intercept were intercepted from networks that were not configured so that such communications were readily accessible to the general public.

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

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

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

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

VII. DEMAND FOR JURY TRIAL

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

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

Dated: November 8, 2010

COHEN MILSTEIN SELLERS & TOLL, PLLC

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

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

Plaintiffs' Co-Lead Counsel

Dated: November 8, 2010

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

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

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

Plaintiffs' Liaison Counsel