IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

PATRICK KEYES
1115 12th Street, NW
Apartment B-1
Washington, DC 20005

DEEPA ISAC
2615 4th Street, NE
Apt. 303
Washington, DC 20002

and

EDWARD FENN
2858 Lawrence Drive
Falls Church, VA 22042,

on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

GOOGLE, INC.
1600 Amphitheatre Parkway
Mountain View, CA 94043,

Defendant.

Civil Action No.:

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Patrick Keyes, Deepa Isac, and Edward Fenn (collectively, "Plaintiffs"), individually and on behalf of a Class (defined below) of all others similarly situated, bring this action for damages 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.*, against Defendant Google, Inc. ("Defendant"), and demand a jury trial.

NATURE OF THE CASE

1. Defendant intentionally intercepted electronic communications sent or received on open wireless internet connections ("WiFi connections") by the Class from at least May 25, 2007 through the present, in violation of the Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511, *et seq.*

2. Defendant intercepted the Class members' electronic communications through 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 WiFi network

names (SSID information) and WiFi router numbers (MAC address), which Defendant used not for Google Street View, but instead to improve Defendant's location based services. Importantly, the data also included all or part of any personal e-mails, passwords, videos, audio, documents, and VOIP information (collectively, "payload data") transmitted over Class members' WiFi networks. 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 payload data that the Google Street View vehicles collected is not reasonably accessible by the general public. Indeed, the data, as initially captured by the wireless sniffer, is not readable by members of the public absent the acquisition and use of sophisticated decoding and processing technology. In addition, members of the public did not give their consent to Defendant to collect this data, nor did they have knowledge that Google Street View vehicles have been collecting this data.

6. After the Google Street View vehicles' wireless sniffers sampled, collected, decoded, and analyzed this 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.

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 Defendant has collected and stored Class members' WiFi data, including payload data. Sergey Brin, Defendant's co-founder, candidly stated that his company "screwed up" and that "I'm not going to make any excuses about this." Defendant has admitted that it included code in Google Street View vehicles' data collection systems that its engineers knew would intercept Class members' payload data.

9. The Federal Trade Commission ("FTC") is currently investigating Defendant's conduct. On May 20, 2010, FTC Chairman Jon Leibowitz said, in response to questioning from Senator Susan Collins during a Senate Appropriations Financial Services and General Government Subcommittee, that his agency is "going to take a very, very close look" at Defendant's conduct.

10. 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.

11. Hong Kong's privacy commissioner, Roderick B. Woo, has threatened unspecified sanctions after Defendant did not respond by May 24, 2010 to his request to inspect data collected in the territory by Google Street View vehicles.

12. 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.

13. 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. Representatives Ed Markey (D., Massachusetts) and Joe Barton (R., Texas) of the Committee on Energy and Commerce wrote a letter to the FTC on May 19, 2010, asking the agency to respond by June 2, 2010 to several questions, including whether it was investigating the matter and whether Defendant's conduct violated federal law. In addition, and on information and belief, at least one State Attorney General's office is currently looking into the matter and determining whether to commence an investigation.

14. Privacy organizations also have requested federal governmental action. On May 18, 2010, Marc Rotenberg, the Director of the Electronic Privacy Information Center ("EPIC"), wrote a letter to the Federal Communications Commission ("FCC") urging it to open an investigation of Defendant, remarking that "[b]y intercepting and recording unencrypted Wi-Fi transmissions, it is very likely that [Defendant] violated the federal Wiretap Act."

15. Soon after the public outcry and calls for governmental investigation began, Defendant announced that it had grounded its Google Street View vehicles and segregated the WiFi data that the vehicles collected, which it then disconnected to make inaccessible. It also decided that given the concerns raised, it would stop the Google Street View vehicles collecting WiFi network data entirely.

16. As a result of Defendant's unlawful conduct, Plaintiffs, on behalf of themselves and members of the Class, brings this action to recover statutory damages, punitive damages, equitable relief, and attorneys' fees and costs under 18 U.S.C. § 2520.

JURISDICTION AND VENUE

17. 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*.

18. 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 Plaintiffs and a substantial number of Class members within this District; (d) Defendant maintains an office in this District; and (e) Plaintiffs Patrick Keyes and Deepa Isac reside within and are citizens of this District.

PARTIES

Plaintiffs

19. Plaintiff Patrick Keyes is an individual that resides within and is a citizen of Washington, D.C. From September 2007 until February 2010, Plaintiff used and maintained a WiFi connection at Plaintiff's home. Plaintiff used the WiFi connection to send and receive various types of private payload data. On information and belief, a Google Street View vehicle has collected, and Defendant has decoded and stored, data from Plaintiff's WiFi connection, including payload data, on at least one occasion.

20. Plaintiff Deepa Isac is an individual that resides within and is a citizen of Washington, D.C. Since 2008, Plaintiff has used and maintained a WiFi connection at Plaintiff's home. Plaintiff used the WiFi connection to send and receive various types of

private payload data. On information and belief, a Google Street View vehicle has collected, and Defendant has decoded and stored, data from Plaintiff's WiFi connection, including payload data, on at least one occasion.

21. Plaintiff Edward Fenn is an individual that resides within and is a citizen of Virginia. From Fall 2007 until December 2009, Plaintiff used and maintained a WiFi connection at Plaintiff's home. Plaintiff used the WiFi connection to send and receive various types of private payload data. On information and belief, a Google Street View vehicle has collected, and Defendant has decoded and stored, data from Plaintiff's WiFi connection, including payload data, on at least one occasion.

Defendant

22. Defendant Google, Inc. ("Defendant") is a Delaware corporation with its principal place of business in Mountain View, California. It also has an office in, among various locations in the United States and worldwide, Washington, D.C., which is housed on the second floor of 1101 New York Avenue, N.W. 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.

FACTUAL ALLEGATIONS

Defendant's Business and Culture

23. 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."

24. Defendant generates billions of dollars per year, primarily from advertising. AdWords is Defendant's flagship advertising product and main source of revenue. In AdWords, advertisers specify the words that should trigger their ads. When a user searches Defendant's search engine, ads for relevant words are shown as "sponsored links" on the right side of the screen, and sometimes above the main search results. Defendant markets this service to advertisers by employing users' personal information, including the contents of e-mails, browsing history, and other personalized metrics, to provide advertisers with the most targeted data possible that tend to reveal user characteristics and preferences.

25. Defendant is widely-recognized to employ some of the best and brightest 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."

26. 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[.]"

27. More so 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.

Privacy Concerns Over Defendant's Practices

28. 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.

29. On March 17, 2009, EPIC asked the FTC to investigate Defendant's so-called cloud computing services, including Gmail and Google Docs. In its petition, EPIC asked the FTC to assess the privacy and security safeguards used by Defendant's online applications and determine 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.

30. In February 2010, Defendant unveiled Buzz, a social networking service featuring a Gmail add-on that automatically exposed users' most frequent e-mail and chat contacts to the general public. Soon thereafter, EPIC filed a complaint with the FTC. 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 law.

31. The privacy concerns, however, largely appear to have fallen on deaf ears. Defendant's CEO, Eric Schmidt, squarely has dismissed such 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."

32. Defendant's conduct regarding 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."

33. 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."

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

35. 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."

36. 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)."

Google Street View

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

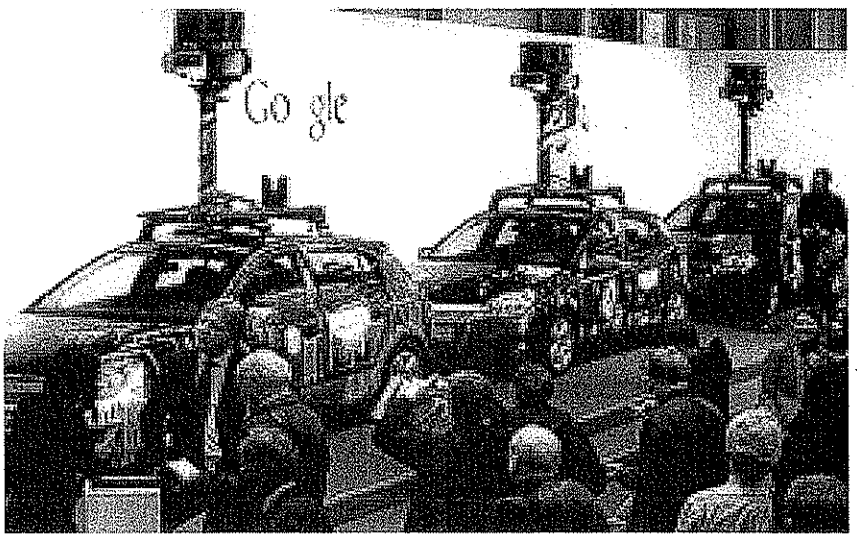
38. Google Street View is a technology featured in Defendant's Google Maps and Google Earth products that offers panoramic views from various positions along many streets across the globe.

39. Defendant first launched Google Street View on May 25, 2007 in several select cities across the United States. Since that time, Google Street View gradually 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. On April 16, 2008, Google Street View was fully integrated into Google Earth 4.3.

40. Google Street View displays images taken from a fleet of specially adapted cars known as Google Street View vehicles. On the top of each Google Street View vehicle are placed nine directional cameras, which provide 360 degree views, and include GPS units for positioning, three laser range scanners for the measuring of up to 50 meters 180 degrees in front of the car, and antennas for scanning 3G/GSM/WiFi hotspots.

41. The antennas placed on top of the Google Street View vehicles receive signals, as well as all other types of data, broadcast through WiFi connections. The development and features of the data collection system that the antennas utilized is described below.

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



43. 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 placed on top of Google Street View vehicles also are placed on Google Trikes.

Development and Implementation of Google Street View Data Collection System

44. Before Google Street View vehicles first hit the streets in mid-2007, Defendant was hard at work developing the data collection system that would be utilized by each vehicle's antenna to collect WiFi data.

45. 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 commonly called a packet analyzer, wireless sniffer, network analyzer, packet sniffer, or protocol analyzer.

46. 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.

47. 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 technology.

48. The data, as initially captured by the wireless sniffer, is not readable by members of the public absent sophisticated decoding and processing technology. Thus, the Class members' payload data is not reasonably accessible by the general public.

49. When Defendant's engineers created the data collection system for its Google Street View vehicles, they intentionally included wireless sniffers that sampled, collected, decoded, and analyzed all types of data broadcast over Class members' WiFi connections. The data collection system that the engineers developed was approved by Defendant before authorizing its inclusion in the Google Street View vehicles and setting them off into the world to obtain information.

50. The data that the Google Street View vehicles collected included Class members' SSID information and MAC address, which Defendant used not for Google Street View, but instead to improve Defendant's location-based user services, as well as services provided by Defendant's Geo Location API.

51. Importantly, however, the collected data also included payload data—*i.e.*, all or part of any personal e-mails, passwords, videos, audio, documents, and VOIP information—transmitted over Class members' WiFi networks.

52. On information and belief, hundreds, if not thousands, of Defendant's employees across the world, including the United States, have access to data maintained on Defendant's servers, including the payload data of Class members that Google Street View vehicles have collected since mid-2007.

53. Significantly, Defendant's engineers did not have to use packet sniffers to retrieve the SSID and MAC address information in the first place. Rather, they had other available options to obtain user's open WiFi data. One approach, known as active scanning, only seeks out WiFi access points, but nothing else, such as payload data. The other approach, known as passive sniffing, is what Defendant chose to use. Passive sniffing picks up all of the data travelling over WiFi connections, including payload data.

54. As Ted Morgan, CEO and co-founder of Skyhook Wireless, stated in a May 18, 2010 *Motley Fool* article, "when you are doing the passive sniffing you have to make sure you are not accessing private network messages. It's not a hard thing to do; you just do not record those messages."

55. Skyhook, which has used active scanning since 2003 to collect data on WiFi networks to feed the database behind the location-finding software that it licenses to mobile device makers like Apple, Motorola, and Dell, has never employed passive sniffing, in part because of the privacy challenges, according to Morgan.

56. Morgan further added to *Motley Fool*: "We feel very comfortable with the data we're collecting, and it also keeps us from ever having to be perceived like we're in the kind of situation that Google's in. It's actually impossible, with the approach we take right now, to observe or capture any private network data. Nor would it be possible for Google to record such data completely by accident. At the engineering level it's very easy to know whether you are capturing this data or not."

57. Defendant never publicly disclosed, until early May 2010, that it had been using Google Street View vehicles to obtain WiFi data, as opposed to simply collecting street view images to post on its Google Maps and Google Earth services. And given the

only publicly revealed function that Google Street View vehicles employed, namely obtaining street level images for inclusion on Defendant's internet services, members of the general public had no reason to think otherwise until recently.

Defendant's Admissions Regarding Interception of Payload Data

58. After Defendant's Google Street View vehicle wireless sniffers sampled, collected, decoded, and analyzed this data, Defendant stored the data on its servers.

59. Defendant admitted very recently—on May 14, 2010—that it has collected and stored data obtained from WiFi connections around the world, including the United States, through its Google Street View vehicles.

60. Defendant's admission came about only in response to a full audit of its WiFi data that Peter Scharr, the German Commissioner for Data Protection and Freedom of Information, initiated in light of privacy concerns over Google Street View.

61. Several high-level representatives of Defendant have admitted that Defendant has indeed collected and stored Class members' WiFi data, including payload data.

62. According to the May 21, 2010 edition of *Businessweek* online, Sergey Brin, Defendant's co-founder, candidly stated at a news conference that his company "screwed up" and that "I'm not going to make any excuses about this."

63. By intentionally developing code for a data collection system that would capture payload data, and by approving the system's inclusion in the Google Street View data collection system that would be used to gather WiFi data, Defendant intentionally intercepted Class members' open WiFi data, including payload data.

Federal Trade Commission Investigation

64. The FTC is currently investigating Defendant's conduct. On May 20, 2010, FTC Chairman Jon Leibowitz was questioned by Senator Susan Collins during a Senate Appropriations Financial Services and General Government Subcommittee on the FTC's budget. When Collins asked Leibowitz if the FTC was investigating the matter, he responded that "while the agency does not comment on investigations until they are over, I can certainly tell you, we're going to take a very, very close look" at Defendant's conduct. Leibowitz further noted: "Obviously this is just one example . . . of why consumers have very serious privacy concerns about data that's being collected. So we are going to take a look at it. Absolutely."

Foreign Governmental Investigations

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

66. 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*. "We are absolutely at an early stage," Wilhelm Möllers, a spokesman for the Hamburg prosecutor's office, said in an interview. "This isn't something that will be wrapped up in two or three weeks. We have to analyze whether there is reason to file criminal charges."

67. German prosecutors are investigating some employees in Defendant's German unit, based in Hamburg, on suspicion of criminal data capture, according to a *Bloomberg* article from May 20, 2010.

68. German data protection officials set a May 26, 2010 deadline for Defendant to produce a hard drive from one of its Google Street View vehicles. According to the May 27, 2010 edition of *The New York Times*, Defendant said that it was unable to comply with the deadline to hand over the data it had collected. The Hamburg data protection supervisor, Johannes Caspar, expressed his disappointment, proclaiming that "there is no apparent reason to still withhold the data from us." As of the date of this Complaint, Defendant apparently still has not complied with this request.

69. According to the Associated Press, on May 15, 2010, Germany's consumer protection minister, 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."

70. The Italian data protection agency announced on May 19, 2010 that it is 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, and where the data was stored. That agency also is inquiring whether Defendant shared the data with third parties.

71. That same day, the Spanish data protection agency also ordered the commencement of an investigation into whether Defendant violated laws governing personal data. That agency said that Defendant's conduct could violate the Organic Data Protection Act, and is asking that Defendant block the traffic data associated with the wireless networks gathered in that country.

72. The French National Commission on Computing and Liberty reported that it would begin investigating Defendant. Noting Defendant's admission that it had collected Wi-Fi traffic, the French agency said on May 19, 2010: "This collection was

not mentioned in Google's declaration to the [agency]. 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."

73. The Czech Office for Personal Data Protection has been looking into potential issues with Google Street View since April 2010, as reported in *Bloomberg*'s May 20, 2010 edition. The office sent a set of conditions to Defendant within the last couple of weeks on what it must do to comply with national privacy protection law.

74. The European Union also has weighed in on Defendant's actions, with EU Justice Commissioner Viviane Reding pointedly stating that "[i]t is not acceptable that a company operating in the EU does not respect EU rules."

75. Hong Kong's privacy commissioner, Roderick B. Woo, has threatened unspecified sanctions after Defendant did not respond to his request to inspect data collected in the territory by Google Street View vehicles, according to the May 27, 2010 edition of *The New York Times*. Woo said that Defendant ignored the May 24, 2010 deadline that he gave it to turn over the information. "I am dismayed by Google's apparent lack of sincerity in its handling of this matter," Mr. Woo said in a statement. "I do not see that Google is taking the matter seriously enough. Unless some remedial measures are taken by Google promptly, I shall have to consider escalating the situation and resort to more assertive action."

76. 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, according to a May 26, 2010 article from the online *Telegraph.co.uk*. According to the same article, Conroy 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.

Calls for Governmental Investigation in the United States

77. The alarm and outcry over Defendant's conduct has not been confined to foreign nations.

78. On May 19, 2010, Representatives Ed Markey (D., Massachusetts) and Joe Barton (R., Texas) of the Committee on Energy and Commerce wrote a letter to the FTC. In that letter, the Congressmen noted that Defendant "has acknowledged it collected private email and Internet surfing data, but it has not yet clarified the extent or nature of the data collected." They went on to request the FTC's response, by June 2, 2010, to the following questions:

> 1. Is the Federal Trade Commission (FTC) investigating this matter?
>
> 2. What is the Commission's understanding of the type and nature of information collected and how is the captured data stored? Who had access to this data?
>
> 3. Do [Defendant's] data collection practices with respect to Wi-Fi networks violate the public's reasonable expectation of privacy? Did [Defendant] collect passwords associated with Internet usage by consumers?
>
> 4. Do Google's actions form the basis of an unfair or deceptive act or practice that constitutes harm to consumers? Please explain your response.
>
> 5. Are [Defendant's] actions illegal under Federal law? If these allegations warrant Commission action, does the Commission believe it currently has authority to take necessary action? If not, please describe legislative language you would recommend to enable the Commission to act appropriately.

79. On information and belief, at least one State Attorney General's office is looking into Defendant's conduct and currently contemplating the initiation of an investigation.

80. Non-profit privacy organizations in the United States also have requested governmental action and voiced significant concern over Defendant's Google Street View practices.

81. On May 18, 2010, Marc Rotenberg, the Director of EPIC, wrote a letter to the FCC urging it to open an investigation of Defendant. In the letter, Rotenberg wrote that "[w]e believe that the Commission should now turn its attention to the significant communications privacy issues arising from Google Street View," which he characterized as "extraordinary." He stated that "[b]y intercepting and recording unencrypted Wi-Fi transmissions"—which Defendant "never disclosed"—"it is very likely that [Defendant] violated the federal Wiretap Act."

Defendant Grounds Google Street View

82. Soon after the governmental investigations and public outcry began, Defendant announced that it had grounded its Google Street View vehicles and segregated the WiFi data that the vehicles collected, which it then disconnected to make inaccessible. It also decided that given the concerns raised, it would stop the Google Street View vehicles collecting WiFi network data entirely.

83. Defendant has offered to destroy the intercepted WiFi data, but has not allowed regulators to see and verify what it has collected. In particular, Defendant has destroyed data collected in Denmark, Ireland and Austria at the request of local regulators. But eight other European countries—Britain, Germany, France, Spain, Italy,

the Czech Republic, Switzerland and Belgium—have asked Defendant to retain data collected in those nations, which may be used as evidence in future legal proceedings.

TOLLING AND FRAUDULENT CONCEALMENT

84. 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 announced that it had been collecting and storing the Class members' open WiFi data, including payload data, via Google Street View.

85. Because Defendant's conduct was kept secret until May 14, 2010, Plaintiff sand members of the Class before that time were unaware of Defendant's unlawful conduct alleged herein.

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

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

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

89. 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 techniques of secrecy employed by Defendant to avoid detection.

90. 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.

91. 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.

92. 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.

CLASS ACTION ALLEGATIONS

93. Plaintiffs bring this action on behalf of themselves and as a class action under Rule 23(a) and (b)(3) of the Federal Rules of Civil Procedure on behalf of the following class (the "Class"):

> All persons in the United States whose electronic communications sent or received on open wireless internet connections ("WiFi connections") were intentionally intercepted by Defendant's Google Street View vehicles from at least May 25, 2007 through the present. Excluded from the Class are Defendant, any of its related companies, subsidiaries and affiliates, and federal governmental entities and instrumentalities.

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

95. There are questions of law and fact common to the Class, including:

(a) Whether Defendant intentionally intercepted 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 Class under 18 U.S.C. § 2520;

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

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

96. Plaintiffs' claims are typical of the claims of Class members, and Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs and all members of the 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 Class members. Plaintiffs' interests are coincident with, and not antagonistic to, those of the other Class members.

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

98. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications, establishing incompatible standards of conduct for Defendant.

99. The questions of law and fact common to the members of the Class predominate over any questions affecting only individual members.

100. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The Class is 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.

CAUSE OF ACTION

101. Plaintiffs incorporate herein and reallege each allegation set forth in the previous paragraphs.

102. Beginning at least as early as May 25, 2007, and continuing through the present, Defendant intentionally intercepted Class members' electronic communications sent or received on their WiFi connections, and thus violated 18 U.S.C. § 2511, *et seq.*

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

(a) Statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000;

(b) Punitive damages in an amount to be determined by the jury;

(c) Equitable or declaratory relief as is deemed appropriate; and

(d) Reasonable attorneys' fees and other litigation costs reasonably incurred.

DEMAND FOR JURY TRIAL

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

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)(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 judgment be entered for Plaintiffs and Class members against Defendant for statutory damages as provided in 18 U.S.C. § 2520;

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

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

E. That Plaintiffs and the Class recover their costs of the suit, including attorneys' fees, as provided by 18 U.S.C. § 2520.

F. That Defendant be enjoined from continuing to engage in the alleged conduct..

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

Dated: May 28, 2010

Daniel A. Small /ce

Daniel A. Small (Bar No. 465094)
Kit A. Pierson (Bar No. 398123)
Benjamin D. Brown (Bar No. 495836)
Victoria S. Nugent (Bar No. 470800)
Christopher J. Cormier (Bar No. 496384)
David Young (Bar No. 980929)
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue, NW
Suite 500 West
Washington, DC 20005
Telephone: 202-408-4600
Facsimle: 202-408-4699
E-mail:dsmall@cohenmilstein.com

kpierson@cohenmilstein.com
bbrown@cohenmilstein.com
vnugent@cohenmilstein.com
ccormier@cohenmilstein.com
dyoung@cohenmilstein.com

George F. Farah (Bar No. 992638)
COHEN MILSTEIN SELLERS & TOLL PLLC
88 Pine Street
14th Floor
New York, NY 10005
Telephone: 212-838-7797
Facsimle: 212-838-7745
E-mail:gfarah@cohenmilstein.com

Steven F. Benz (Bar No. 428026)
Michael J. Guzman (Bar No. 445412)
KELLOGG, HUBER, HANSEN, TODD, EVANS & FIGEL, P.L.L.C.
Sumner Square
1615 M Street, N.W., Suite 400
Washington, DC 20036
Telephone: 202-326-7900
Facsimile: 202-326-7999
E-mail: sbenz@khhte.com
mguzman@khhte.com

Harvey Rosenfield
Pamela Pressley
Todd M. Foreman
CONSUMER WATCHDOG
1750 Ocean Park Blvd.,
Santa Monica, California 90405
Telephone: 310-392-0522
Facsimile: 310-392-8874
E-mail: harvey@consumerwatchdog.org
pamela@consumerwatchog.org
todd@consumerwatchdog.org

Counsel for Plaintiffs and Proposed Class