

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

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

ERIC MYHRE, on behalf of himself and all )  
others similarly situated, )  
 )  
Plaintiff )  
 )  
vs. )  
 )  
GOOGLE, INC. )  
 )  
Defendant. )  
 )  
 )  
 )  
 )

No.  
  
CLASS ACTION COMPLAINT  
  
JURY TRIAL DEMANDED

Plaintiff Eric Myhre (“Plaintiff”), 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

1 Communications Privacy Act of 1986, 18 U.S.C. § 2511, *et seq.*

2 2. Defendant intercepted the Class members' electronic communications through its  
3 Google Street View vehicles. Google Street View is a web-based and web-accessed technology  
4 featured in Google Maps and Google Earth that displays images taken from a fleet of specially  
5 adapted cars, known as Google Street Vehicles, and provides panoramic views of homes, offices  
6 and other buildings to users from various positions along many streets world-wide. Defendant  
7 launched Google Street View on May 25, 2007 in the United States, and has since expanded this  
8 offering to more than 30 nations.  
9

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

13 4. When Defendant's engineers created the data collection system for its Google  
14 Street View vehicles, most commonly known as a packet analyzer or wireless sniffer, they  
15 intentionally included computer code in the system that was designed to and did sample, collect,  
16 decode, and analyze all types of data sent and received over the WiFi connections of Class  
17 members. This data included Class members' unique WiFi network names (SSID information)  
18 and WiFi router numbers (MAC address), which Defendant used not for Google Street View, but  
19 instead to improve Defendant's location based services. Importantly, the data also included all  
20 or part of any personal e-mails, passwords, videos, audio, documents, and VOIP information  
21 (collectively, "payload data") transmitted over Class members' WiFi networks. The  
22 employment of packet sniffers, and thus the underlying code, was approved by Defendant's  
23 project team leaders before it was included in the Google Street View vehicles.  
24

25 5. The payload data that the Google Street View vehicles collected is not reasonably  
26

1 accessible by the general public. Indeed, the data, as initially captured by the wireless sniffer, is  
2 not readable by members of the public absent the acquisition and use of sophisticated decoding  
3 and processing technology. In addition, members of the public did not give their consent to  
4 Defendant to collect this data, nor did they have knowledge that Google Street View vehicles  
5 have been collecting this data.

6           6. After the Google Street View vehicles' wireless sniffers sampled, collected,  
7 decoded, and analyzed this data, Defendant stored the data on its servers. Defendant has  
8 admitted that it has collected and stored data from WiFi connections around the world, including  
9 the United States.

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

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

20           9. The Federal Trade Commission ("FTC") is currently investigating Defendant's  
21 conduct. On May 20, 2010, FTC Chairman Jon Leibowitz said, in response to questioning from  
22 Senator Susan Collins during a Senate Appropriations Financial Services and General  
23 Government Subcommittee, that his agency is "going to take a very, very close look" at  
24  
25  
26

1 Defendant's conduct.

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

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

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

14 13. The alarm and outcry over Defendant's conduct has not been limited to overseas.  
15 United States Congressmen have requested governmental investigation into Defendant's  
16 conduct. Representatives Ed Markey (D., Massachusetts) and Joe Barton (R., Texas) of the  
17 Committee on Energy and Commerce wrote a letter to the FTC on May 19, 2010, asking the  
18 agency to respond by June 2, 2010 to several questions, including whether it was investigating  
19 the matter and whether Defendant's conduct violated federal law. In addition, and on  
20 information and belief, at least one State Attorney General's office is currently looking into the  
21 matter and determining whether to commence an investigation.

22 14. Privacy organizations also have requested federal governmental action. On May  
23 18, 2010, Marc Rotenberg, the Director of the Electronic Privacy Information Center ("EPIC"),  
24

1 wrote a letter to the Federal Communications Commission (“FCC”) urging it to open an  
2 investigation of Defendant, remarking that “[b]y intercepting and recording unencrypted Wi-Fi  
3 transmissions, it is very likely that [Defendant] violated the federal Wiretap Act.”

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

9  
10 16. As a result of Defendant’s unlawful conduct, Plaintiff, on behalf of himself and  
11 members of the Class, brings this action to recover statutory damages, punitive damages,  
12 equitable relief, and attorneys’ fees and costs under 18 U.S.C. § 2520.

13 **JURISDICTION AND VENUE**

14 17. This Court has jurisdiction under 28 U.S.C. § 1331 because Plaintiff has alleged  
15 the violation of a federal statute, 18 U.S.C. § 2511, *et seq.*

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

23 **PARTIES**

24  
25 19. Plaintiff Eric Myhre is a United States citizen and resident of Seattle, Washington.  
26 Plaintiff used and maintained an unencrypted wireless internet connection at his home, which he

1 used to send and receive various types of private data. Pictures of his home appear on Google's  
2 Street View maps. On information and belief, a Google Street View vehicle has intercepted and  
3 collected, and Google has stored, data from Plaintiff's WiFi connection.

4 20. Defendant Google, Inc. is a Delaware corporation with its principal place of  
5 business in Mountain View, California.

6 **FACTUAL ALLEGATIONS**

7 **Defendant's Business and Culture**

8  
9 21. Defendant states on its website that its name "reflects the immense volume of  
10 information that exists, and the scope of [its] mission: to organize the world's information and  
11 make it universally accessible and useful." Defendant also boasts on its website of its "superior  
12 search technology," and that "[a]s with its technology, [it] has chosen to ignore conventional  
13 wisdom in designing its business."

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

22  
23  
24 23. Defendant is widely-recognized to employ some of the best and brightest in the  
25 high-technology industry. On its website section titled "Google Management," Defendant lays  
26 claim to "a management team that represents some of the most experienced technology

1 professionals in the industry.”

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

8  
9 25. More so than other companies, even including those in the high-technology  
10 sector, engineers play a pivotal and ubiquitous role in Defendant’s daily operations and overall  
11 strategy. Indeed, observers have commented on Defendant’s engineering-centric culture, and  
12 have remarked that Defendant is run by its engineers.

13 **Privacy Concerns Over Defendant’s Practices**

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

17  
18 27. On March 17, 2009, EPIC asked the FTC to investigate Defendant’s so-called  
19 cloud computing services, including Gmail and Google Docs. In its petition, EPIC asked the  
20 FTC to assess the privacy and security safeguards used by Defendant’s online applications and  
21 determine whether the company had properly represented these safeguards. EPIC’s petition  
22 arose, in part, from Defendant’s inadvertent sharing of certain Google Docs files with users  
23 unauthorized to view them, despite Defendant’s representations on its homepage that its services  
24 were private and secure.

25  
26 28. In February 2010, Defendant unveiled Buzz, a social networking service featuring

1 a Gmail add-on that automatically exposed users' most frequent e-mail and chat contacts to the  
2 general public. Soon thereafter, EPIC filed a complaint with the FTC. EPIC alleged that the  
3 service violated user expectations, diminished user privacy, and contradicted Defendant's  
4 privacy policy. EPIC also noted that Buzz may have violated federal wiretap law.

5 29. The privacy concerns, however, largely appear to have fallen on deaf ears.  
6 Defendant's CEO, Eric Schmidt, squarely has dismissed such concerns, stating in a December  
7 2009 CNBC interview that "[i]f you have something that you don't want anyone to know, maybe  
8 you shouldn't be doing it in the first place."

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

15 31. Privacy authorities from 10 countries—including Canada, France, Germany,  
16 Ireland, Israel, Italy, the Netherlands, New Zealand, Spain and the United Kingdom—issued a  
17 forcefully worded letter to Defendant on April 19, 2010 about its privacy practices in general and  
18 regarding Google Buzz and Google Street View in particular. The group said that Defendant too  
19 often had "failed to take adequate account of privacy considerations when launching new  
20 services," and that it needed to build privacy safeguards and controls directly into new products  
21 as they were being designed, rather than trying to apply them later. Among the minimum  
22 suggested safeguards urged was "collecting and processing only the minimum amount of  
23 personal information necessary to achieve the identified purpose of the product or service."  
24  
25  
26



1           32. Defendant’s conduct also has caught the attention of numerous privacy  
2 organizations, which have given Defendant abysmal marks.

3           33. Public Information Research, Inc. (“PIR”), a non-profit organization, “specializes  
4 in monitoring privacy violations on the web.” In 2002, PIR launched a website called Google  
5 Watch, which advertised itself as “a look at Google’s monopoly, algorithms, and privacy issues.”  
6 The site questioned Google’s storage of cookies, which in 2007 had a life span exceeding 32  
7 years and incorporated a unique ID that enabled the creation of a user data log. In February  
8 2003, Google Watch nominated Defendant for a “Big Brother Award,” calling Defendant a  
9 “privacy time bomb.”  
10

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

### Google Street View

24           35. Defendant’s historically nonchalant attitude towards privacy concerns has carried  
25 through, unfortunately, to its development and implementation of Google Street View.  
26

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

4 37. Defendant first launched Google Street View on May 25, 2007 in several select  
5 cities across the United States. Since that time, Google Street View gradually has expanded to  
6 include more cities and rural areas across the United States and worldwide, and Google Street  
7 View now is offered in more than 30 countries. On April 16, 2008, Google Street View was  
8 fully integrated into Google Earth 4.3.

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

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

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

21 **Development and Implementation of Google Street View Data Collection System**

22 41. Before Google Street View vehicles first hit the streets in mid-2007, Defendant  
23 was hard at work developing the data collection system that would be utilized by each vehicle's  
24  
25  
26

1 antenna to collect WiFi data.

2 42. In 2006, Defendant's engineers intentionally created a data collection system to  
3 include code that sampled and collected, decoded and analyzed all types of data broadcast  
4 through WiFi connections. This type of system is commonly called a packet analyzer, wireless  
5 sniffer, network analyzer, packet sniffer, or protocol analyzer.

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

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

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

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

20 47. The data that the Google Street View vehicles collected included Class members'  
21 SSID information and MAC address, which Defendant used not for Google Street View, but  
22 instead to improve Defendant's location-based user services, as well as services provided by  
23 Defendant's Geo Location API.  
24  
25  
26

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

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

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

14 51. As Ted Morgan, CEO and co-founder of Skyhook Wireless, stated in a May 18,  
15 2010 *Motley Fool* article, “when you are doing the passive sniffing you have to make sure you  
16 are not accessing private network messages. It’s not a hard thing to do; you just do not record  
17 those messages.”

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

22 53. Morgan further added to *Motley Fool*: “We feel very comfortable with the data  
23 we’re collecting, and it also keeps us from ever having to be perceived like we’re in the kind of  
24

1 situation that Google's in. It's actually impossible, with the approach we take right now, to  
2 observe or capture any private network data. Nor would it be possible for Google to record such  
3 data completely by accident. At the engineering level it's very easy to know whether you are  
4 capturing this data or not."

5 54. Defendant never publicly disclosed, until early May 2010, that it had been using  
6 Google Street View vehicles to obtain WiFi data, as opposed to simply collecting street view  
7 images to post on its Google Maps and Google Earth services. And given the only publicly  
8 revealed function that Google Street View vehicles employed, namely obtaining street level  
9 images for inclusion on Defendant's internet services, members of the general public had no  
10 reason to think otherwise until recently.

11  
12 **Defendant's Admissions Regarding Interception of Payload Data**

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

15  
16 56. Defendant admitted very recently—on May 14, 2010—that it has collected and  
17 stored data obtained from WiFi connections around the world, including the United States,  
18 through its Google Street View vehicles.

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

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

24 59. According to the May 21, 2010 edition of *Businessweek* online, Sergey Brin,  
25 Defendant's co-founder, candidly stated at a news conference that his company "screwed up"  
26

1 and that “I’m not going to make any excuses about this.”

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

6 **Federal Trade Commission Investigation**

7  
8 61. The FTC is currently investigating Defendant’s conduct. On May 20, 2010, FTC  
9 Chairman Jon Leibowitz was questioned by Senator Susan Collins during a Senate  
10 Appropriations Financial Services and General Government Subcommittee on the FTC’s budget.  
11 When Collins asked Leibowitz if the FTC was investigating the matter, he responded that “while  
12 the agency does not comment on investigations until they are over, I can certainly tell you, we’re  
13 going to take a very, very close look” at Defendant’s conduct. Leibowitz further noted:  
14 “Obviously this is just one example . . . of why consumers have very serious privacy concerns  
15 about data that’s being collected. So we are going to take a look at it. Absolutely.”

16  
17 **Foreign Governmental Investigations**

18 62. Defendant’s admission also has caused numerous foreign governments to take  
19 note, with several governmental agencies and authorities already having initiated investigations  
20 into Defendant’s conduct.

21 63. On May 19, 2010, German prosecutors based in Hamburg announced the opening  
22 of a criminal investigation into Defendant’s conduct, according to *The New York Times*. “We are  
23 absolutely at an early stage,” Wilhelm Möllers, a spokesman for the Hamburg prosecutor’s  
24 office, said in an interview. “This isn’t something that will be wrapped up in two or three weeks.  
25 We have to analyze whether there is reason to file criminal charges.”  
26

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

4           65.     German data protection officials set a May 26, 2010 deadline for Defendant to  
5 produce a hard drive from one of its Google Street View vehicles. According to the May 27,  
6 2010 edition of *The New York Times*, Defendant said that it was unable to comply with the  
7 deadline to hand over the data it had collected. The Hamburg data protection supervisor,  
8 Johannes Caspar, expressed his disappointment, proclaiming that "there is no apparent reason to  
9 still withhold the data from us." As of the date of this Complaint, Defendant apparently still has  
10 not complied with this request.

11           66.     According to the Associated Press, on May 15, 2010, Germany's consumer  
12 protection minister, Ilse Aigner, referred to Defendant's conduct as "alarming," and remarked  
13 that "[a]ccording to the information available to us so far, [Defendant] has for years penetrated  
14 private networks, apparently illegally."

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

19           68.     That same day, the Spanish data protection agency also ordered the  
20 commencement of an investigation into whether Defendant violated laws governing personal  
21 data. That agency said that Defendant's conduct could violate the Organic Data Protection Act,  
22 and is asking that Defendant block the traffic data associated with the wireless networks gathered  
23 in that country.  
24  
25  
26

1           69.     The French National Commission on Computing and Liberty reported that it  
2 would begin investigating Defendant. Noting Defendant's admission that it had collected Wi-Fi  
3 traffic, the French agency said on May 19, 2010: "This collection was not mentioned in  
4 Google's declaration to the [agency]. That's why the Commission is currently conducting a  
5 review of Google, in order to obtain all the information on this case and decide what action to  
6 take."

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

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

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

22           73.     Australia's minister for broadband, communications and the digital economy,  
23 Stephen Conroy, has told an Australian senate committee that Defendant deliberately decided to  
24  
25  
26



1 collect payload data, according to a May 26, 2010 article from the online *Telegraph.co.uk*.  
2 According to the same article, Conroy said that Defendant's claims that it collected data by  
3 mistake were wrong, and that Defendant deliberately wrote a computer code designed to gather  
4 the private information.

5 **Calls for Governmental Investigation in the United States**

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

8  
9 75. On May 19, 2010, Representatives Ed Markey (D., Massachusetts) and Joe  
10 Barton (R., Texas) of the Committee on Energy and Commerce wrote a letter to the FTC. In that  
11 letter, the Congressmen noted that Defendant "has acknowledged it collected private email and  
12 Internet surfing data, but it has not yet clarified the extent or nature of the data collected." They  
13 went on to request the FTC's response, by June 2, 2010, to the following questions:

- 14
- 15 ● Is the Federal Trade Commission (FTC) investigating this matter?
  - 16 ● What is the Commission's understanding of the type and nature of information  
17 collected and how is the captured data stored? Who had access to this data?
  - 18 ● Do [Defendant's] data collection practices with respect to Wi-Fi networks violate  
19 the public's reasonable expectation of privacy? Did [Defendant] collect  
20 passwords associated with Internet usage by consumers?
  - 21 ● Do Google's actions form the basis of an unfair or deceptive act or practice that  
22 constitutes harm to consumers? Please explain your response.
- 23  
24  
25  
26

- 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.

76. 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.

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

78. 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**

79. 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.

80. Defendant has offered to destroy the intercepted WiFi data, but has not allowed

1 regulators to see and verify what it has collected. In particular, Defendant has destroyed data  
2 collected in Denmark, Ireland and Austria at the request of local regulators. But eight other  
3 European countries—Britain, Germany, France, Spain, Italy, the Czech Republic, Switzerland  
4 and Belgium—have asked Defendant to retain data collected in those nations, which may be  
5 used as evidence in future legal proceedings.

6 **TOLLING AND FRAUDULENT CONCEALMENT**

7  
8 81. Plaintiff and members of the Class did not discover, and could not have  
9 discovered through the exercise of reasonable diligence, the existence of Defendant's conduct  
10 alleged herein until May 14, 2010, when Defendant first announced that it had been collecting  
11 and storing the Class members' open WiFi data, including payload data, via Google Street View.

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

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

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

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

20 86. Plaintiff and members of the Class could not have discovered Defendant's  
21 conduct at an earlier date by the exercise of reasonable diligence because of the deceptive  
22 practices and techniques of secrecy employed by Defendant to avoid detection.

23 87. None of the facts or information available to Plaintiff and members of the Class  
24 prior to May 14, 2010, if investigated with reasonable diligence, could or would have led to the  
25  
26

1 discovery of Defendant's conduct alleged herein prior to that date.

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

5 89. In addition, the claims of Plaintiff and the Class members did not accrue until  
6 they knew of Defendant's unlawful conduct and corresponding legal violations.  
7

8 **CLASS ACTION ALLEGATIONS**

9 90. Plaintiff brings this action on behalf of themselves and as a class action under  
10 Rule 23(a) and (b)(3) of the Federal Rules of Civil Procedure on behalf of the following class (the  
11 "Class"):

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

18 91. Plaintiff believes that there are tens of thousands, and perhaps millions, of Class  
19 members located throughout the United States, the exact number and their identities being  
20 known by Defendant, making the Class so numerous and geographically dispersed that joinder of  
21 all members is impracticable.

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

- 23 (a) Whether Defendant intentionally intercepted Class members' electronic  
24 communications sent or received on WiFi connections, in violation of 18  
25 U.S.C. § 2511, *et seq.*;
- 26 (b) The appropriate amount of statutory damages that should be awarded to  
the Class under 18 U.S.C. § 2520;

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

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

5 93. Plaintiff's claims are typical of the claims of Class members, and Plaintiff will  
6 fairly and adequately protect the interests of the Class. Plaintiff and all members of the Class are  
7 similarly affected by Defendant's wrongful conduct in violation of the federal wiretap statute in  
8 that their electronic communications transmitted over WiFi connections were intentionally  
9 intercepted by Defendant's Google Street View vehicles. Plaintiff's claims arise out of the same  
10 common course of conduct giving rise to the claims of the other Class members. Plaintiff's interests  
11 are coincident with, and not antagonistic to, those of the other Class members.

12 94. Plaintiff is represented by counsel who is competent and experienced in the  
13 prosecution of class action litigation.

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

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

19 97. A class action is superior to other available methods for the fair and efficient  
20 adjudication of this controversy. The Class is readily definable. Prosecution as a class action will  
21 eliminate the possibility of repetitious litigation. Treatment as a class action will permit a large  
22 number of similarly situated persons to adjudicate their common claims in a single forum  
23 simultaneously, efficiently, and without the duplication of effort and expense that numerous  
24  
25  
26

1 individual actions would engender. This action presents no difficulties in management that  
2 would preclude maintenance as a class action.

3 **CAUSE OF ACTION**

4 98. Plaintiff incorporates herein and realleges each allegation set forth in the previous  
5 paragraphs.

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

9 100. Pursuant to 18 U.S.C. § 2520, Plaintiff and Class members are each entitled to the  
10 following:  
11

- 12 (a) Statutory damages of whichever is the greater of \$100 a day for each day  
13 of violation or \$10,000;  
14 (b) Punitive damages in an amount to be determined by the jury;  
15 (c) Equitable or declaratory relief as is deemed appropriate; and  
16 (d) Reasonable attorney's fees and other litigation costs reasonably incurred.  
17

18 **DEMAND FOR JURY TRIAL**

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

21 **PRAYER FOR RELIEF**

22 WHEREFORE, Plaintiff prays for the following relief:

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

25 B. That Defendant's conduct be adjudged to have violated 18 U.S.C. § 2511, *et seq.*  
26

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

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

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

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

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

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

11 DATED this 9th day of September, 2010.

12  
13  
14  
15 KELLER ROHRBACK L.L.P.

16  
17 By s/ Mark A. Griffin

18 Mark A. Griffin, WSBA #16296  
19 1201 Third Avenue, Suite 3200  
20 Seattle, WA 98101-3052  
21 Tel: (206) 623-1900  
22 Fax: (206) 623-3384  
23 mgriffin@kellerrohrback.com

24 Attorneys for Individual and Representative  
25 Plaintiff Eric Myhre  
26