Rick Klingbeil, OSB #933326
RICK KLINGBEIL, PC
520 SW Sixth, Suite 950
Portland, OR 97204
Ph: (503) 473-8565
rick@klingbeil-law.com

Brady Mertz, OSB #970814, WSB #32558
2285 Liberty St NE
Salem, OR 97301
Ph: (503) 385-0121
brady@bradymertz.com

Brooks Cooper, OSB #941772, WSB #32460
520 SW 6th Ave., Suite 914
Portland, OR 97204
Ph: (971) 645-4433
brooks@bcooper-law.com

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

VICKI VAN VALIN, on behalf of herself and all others similarly situated within the state of Oregon; NEIL MERTZ on behalf of himself and all others similarly situated within the state of Washington; Plaintiffs, v. **GOOGLE INC., a Delaware corporation;** Defendant.	No. CV 10-557 ST **SECOND AMENDED CLASS ACTION ALLEGATION COMPLAINT** **(Common Law Invasion of Privacy; RCW 9.73.030; 18 U.S.C. § 2511; 47 U.S.C. § 605)** **DEMAND FOR JURY TRIAL**

Plaintiffs individually and on behalf of the below-described class amend their first amended complaint, and allege as follows:

NATURE OF THE CASE

1. This is a class action. Plaintiffs, on behalf of themselves and all similarly situated persons seek recovery of monetary damages, penalties, costs, attorney fees, and other relief based on certain acts of defendant, including invasion of their legally protected privacy interests, acquisition of personal and private information without permission or consent, and violation of privacy and security rights granted by the common law of the State of Oregon and Washington, RCW 9.73.030, 18 U.S.C. § 2511, and 47 U.S.C. § 605.

JURISDICTION AND VENUE

2. This court has original jurisdiction over this class action under 18 U.S.C. § 1332(d) the Class Action Fairness Act ("CAFA"). The CAFA explicitly provides for the original jurisdiction of the federal court in any class action in which any member of the class is a citizen of a state different from any Defendant, and where the matter in controversy exceed the sum of $5 million exclusive of interests and costs. Plaintiffs allege that the claims of individual class members in this action exceeds $5 million in the aggregate, exclusive of interest and costs, and that the total number of members of the proposed class is greater than 100, as required by 28 U.S.C. § 1332(d)(2), (5). As set forth below, plaintiffs are citizens of Oregon and Washington, and defendant is a Delaware corporation with its headquarters and main office located in California. This court also has jurisdiction under 28 U.S.C. § 1331 because plaintiffs have alleged a violation of 18 U.S.C. § 2511, et seq.

3. Venue lies within this District pursuant to 28 U.S.C. 1391(b)-(c) in that defendant conducts business in this District; certain acts giving rise to the claims asserted in this Complaint occurred within this District; the actions of Defendants alleged in this Complaint caused damages to plaintiff Van Valin and a substantial number of class members within this District, and plaintiff

Vicki Van Valin resides within this District.

THE PARTIES

4. Plaintiff Vicki Van Valin ("Van Valin") is an individual residing in Oregon. During the class period, Van Valin used and maintained an open wireless internet connection ("wireless connection") at her home. Van Valin used the wireless internet connection to transmit and receive personal and private data, including but not limited to personal emails, personal internet research and viewing, work-related emails, work-related documents, work-related internet research and viewing, credit card information, banking information, personal identification information such as social security numbers, date of birth, medical information, and telephone calls made using a voice over internet (VOIP) protocol.

5. Plaintiff Neil Mertz ("Mertz") is an individual residing in the state of Washington. During the class period, Mertz used and maintained and used an open wireless internet connection ("wireless connection") at his home. Mertz used the wireless internet connection to transmit and receive personal and private data, including but not limited to personal emails, personal internet research and viewing, credit card information, banking information, personal identification information such as social security numbers, date of birth, and medical information.

6. Defendant Google Inc. ("Google") is a multinational public cloud computing and internet search technologies corporation. Google hosts and develops a number of Internet-based services and products. It was first incorporated as a privately held company on September 4, 1998, with its initial public offering to follow on August 19, 2004. Google is a Delaware corporation with its home office in the state of California. The company's stated mission from the outset of its existence has been "to organize the world's information and make it universally accessible and useful."

DEFENDANT'S CONDUCT

7. Google also offers a variety of location-based services, such as Google Latitude, Google Toolbar with My Location, and location aware browsing through the Mozilla Firefox browser using Google Maps. Collectively, the underlying technology is called Google Location Service ("GLS"). Developers, websites, and programs can use GLS to gain access to a user's approximate location. This allows an important business advantage because information, such as mapping, social networking, and advertising can then be keyed to the user's specific location.

8. One of Google's web-based and web-accessed internet services is Google Street View ("GSV"). GSV is a technology featured in the Google Maps and Google Earth products that provides panoramic views from various positions along many streets in the United States and throughout the world. It was launched on May 25, 2007, originally only in several cities in the United States, and has since gradually expanded to include more cities and rural areas throughout the states of Oregon and Washington, the United States, and worldwide. GSV displays images taken from a fleet of specially adapted vehicles ("GSV vehicles"). Areas not accessible by a full-sized vehicle, such as pedestrian areas, narrow streets, alleys and ski resorts are sometimes covered by Google Trikes (tricycles) or a snowmobile.

9. On each of the GSV vehicles there are typically nine directional cameras for 360° views at a height of about 2.5 meters, global positioning system ("GPS") units for obtaining geo-location coordinates, three laser range scanners for the measuring of up to 50 meters 180° in the front of the vehicle. There are also 3G/GSM/Wi-Fi antennas for scanning 3G/GSM and Wi-Fi broadcasts (sometimes called "hotspots") and associated electronic hardware for the interception and storage of wireless signals, electronic communications, and data ("Wireless Data").

10. Beginning in or about 2006, Google generated or incorporated programming code

into the electronic hardware on its GSV vehicles that intercepted all categories of broadcast Wireless Data. This type or class of program is commonly called a packet analyzer, also known as a network analyzer, protocol analyzer or packet sniffer, or for wireless networks, a wireless sniffer ("wireless sniffer"). As data is transmitted from a user's network or computer, and across their wireless access point ("wireless AP"), the sniffer secretly and undetectably captures the Wireless Data, then decodes and analyzes its content according to the appropriate specifications and protocols, or passes the Wireless Data to another program for processing.

11. After Wireless Data has been secretly intercepted by a wireless sniffer in a raw or unparsed format, it must be parsed or decoded from its "raw" format before it becomes readily accessible or can be read in understandable plain text. For example, a study commissioned by Google, and published on June 3, 2010 by Stroz Friedberg, LLC, explained that after interception "the payload - which exists in memory in a non-structured bit stream of ones and zeros -- is written to disk in a serialized format...."; "unencrypted Data frames' bodies pass through memory unparsed and are written to disk in their unparsed format"; and "some frame elements (MAC, SSID, et al.) parsed out. - Others (payload) not inspected and stored in raw format." Because of this, wireless payload data broadcast from an unencrypted wireless AP is reasonably considered and understood to be private, protected information which is scrambled and not readily accessible to the public absent parsing or decoding using specialized software and methods.

12. When Google created the Wireless Data interception and storage systems on its GSV vehicles, it included wireless sniffers and other related software and devices. Google's wireless sniffers intercepted Wireless Data from wireless APs which included: (1) the user's unique or chosen name for their wireless AP (SSID Name), (2) the unique and permanent number assigned by the manufacturer to the user's wireless AP hardware (MAC Address), (3) up to three other available

MAC Addresses for other devices located within the user's home or facility, (4) electronic data and information showing the routing and addressing information transmitted from or to the user's wireless AP and equipment, and (5) electronic communications and data consisting of all or part of any documents, emails, video, audio, VOIP, and other content being sent over the network by the user, commonly called "payload data." Concurrent with interception of the above Wireless Data, Google also obtained the geo-location coordinates from its onboard GPS, then associated that information and the exact time with the intercepted Wireless Data. This created a direct link and association between the content of the intercepted Wireless Data, the location of the home or facility from which it was intercepted, the date and time it was intercepted, the manufacturer and types of various hardware within the user's home or facility, and other intercepted information.

13. Google made a conscious and knowing decision to intercept and store all the Wireless Data obtained, including the payload data. Two programs were used for this purpose by Google. One was Kismet, which intercepted the Wireless Data then passed it to a second program, Gslite. After receiving intercepted Wireless Data from Kismet, Gslite performed some processing on it, and then wrote part or all of it to storage media.

14. When sniffing Wireless Data, Kismet can be configured to either intercept, or ignore payload data. Gslite can similarly be configured to either process and store payload data passed to it by Kismet, or discard it. As configured by Google for use on its GSV vehicles, Kismet was set up to intercept and obtain all payload data, then pass it to the Gslite program. As configured by Google for use on its GSV vehicles, the Gslite program was set up to examine the payload data received from Kismet to determine whether it was encrypted or unencrypted. After examining the payload data, if Gslite determined it was encrypted, and therefore not readable or usable by Google without time and resource intensive decryption, Gslite was configured by Google to discard the payload

data. If the payload data was unencrypted, and therefore readable and usable by Google after decoding and parsing, the payload data was then written to storage media, and later to Google's servers. Google, therefore, made the conscious and knowing decision to configure Kismet to capture payload data, and the conscious and knowing decision to configure Gslite to examine the characteristics of payload data passed to it by Kismet, discard it if it was encrypted and unusable, or record it to storage media if unencrypted and usable.

15. (a) Some class members operated their wireless APs in an unmodified, factory default condition, also known as an open broadcast. Google intercepted all of the above-described Wireless Data from class members with unmodified, open APs, associated it with the geographic location and time data, and recorded all the information onto storage media.

(b) Some class members modified the instruction set within the memory contained in their wireless APs to cause their devices to encrypt portions of their Wireless Data. Google intercepted all of the above-described Wireless Data from those class members, associated it with the geographic location and time data, and recorded all the information, except for the encrypted payload data, onto storage media.

(c) Some class members modified the instruction set within the memory contained in their wireless AP to cause their devices to encrypt portions of their Wireless Data, and to cause their AP to hide or not broadcast their SSID Information in order to make it more difficult for others to discover the existence of their wireless AP. Google intercepted all of the above-described Wireless Data from these class members, associated it with the geographic location and time data, and recorded all the information, except for the encrypted payload data, onto storage media.

16. At various times, Google caused the stored Wireless Data, and associated time and

geographic location data from its GSV vehicles to be stored onto its servers. On information and belief, over the past three years, hundreds if not thousands of Google employees throughout the United States and the world have had access to the Wireless Data and associated information on Google's servers.

17. Users had an expectation of privacy with respect to the Wireless Data collected by Google. Because the GSV packet sniffing and data collection was done in secret, and without requiring the device used by Google to be associated with the user's AP device, users could not, and did not give their consent to Google's activities.

18. On November 26, 2008 United States Patent Application No. 12/315,079, entitled "Wireless Network-Based Location Approximation" was filed with the United States Patent and Trademark Office. On January 28, 2010 Patent Application No. 12/315,079 was published as US 2010/0020776 A1 ('776 Application"). Google Inc. was the assignee of the '776 Application. The '776 Attached is as Exhibit "A."

19. The '776 Application discloses a method devised by Google for gathering, analyzing, and using data sent by users over their wireless APs. One way the data can be gathered, Google claims, is through a wireless receiver, using a sensitive high gain antenna, operating in a "sniffer" mode to obtain all types of data transmitted by a user's wireless AP. The data so gathered, explains Google, can then be analyzed or decoded with an "analyzer program."

20. The '776 Application shows that with data collected from a user's wireless AP, Google can determine, among other things (1) the vendor and model of their wireless AP device, (2) the geographic coordinates, and therefore the location or street address where the wireless AP is located, and (3) the approximate location of the wireless AP within the user's residence or business. The invention also provides the capability for Google, or others with access to the data collected

and analyzed as described by Google, to directly correlate the data with a precise location, such as GPS coordinates or a street address.

21. As disclosed in the '776 Application, the more types and greater the quantity of wireless data intercepted, decoded, and analyzed by Google from any particular user or location, the higher its "confidence level" in the calculated location of that user's wireless AP. Collection, decoding, and analysis of a user's payload data would, therefore, serve to increase the accuracy, value, useability, and marketability of Google's new method for wireless network-based location approximation, and any service that relied upon that method, such as the Google Location Service.

22. The '776 Application also discloses that the confidence level in determining the location of a user's wireless AP can be enhanced or increased by decoding, then analyzing what types of data has been captured (i.e. management frames, control frames, or payload data), then reviewing the decoded data to determine whether it arrived in an intact or corrupted state.

23. The '776 Application also discloses that the receiver or device used to collect the wireless data "may be placed in a vehicle and data may be obtained continuously or at predetermined time increments" and that the rate of speed of the vehicle "may be factored into the analysis."

24. Google has employed one or more of the methods disclosed in the '776 Application to collect, decode, analyze, store, and / or make beneficial use of Wireless Data it collected from plaintiffs and class members.

PLAINTIFF VAN VALIN'S EXPERIENCE

25. Since the time Google began collecting users' Wireless Data with its GSV vehicles, plaintiff Van Valin has consistently maintained an open wireless internet connection at her residence.

26. Van Valin's residence is located on and adjacent to a street for which a GSV vehicle has collected data on at least one occasion since May 25, 2007.

27. Van Valin works in the high technology field, and works from her home over her internet-connected computer a substantial amount of time. In connection with her work and home life, Van Valin transmits and receives a substantial amount of Wireless Data. A significant amount of the Wireless Data was also subject to her employer's non-disclosure and security regulations.

28. Unauthorized access to Van Valin's personal and work-related Wireless Data invades her objectively reasonable expectations of privacy, and invades her rights to privacy.

29. On information and belief, a GSV vehicle has collected, and defendant has stored, and decoded Van Valin's Wireless Data on at least one occasion.

PLAINTIFF MERTZ'S EXPERIENCE

30. Since the time Google began collecting users' Wireless Data with its GSV vehicles, plaintiff Mertz has consistently maintained an open wireless internet connection at his residence.

31. Mertz's residence is located on a street for which a GSV vehicle has collected data on at least one occasion since May 25, 2007.

32. Mertz transmits and receives a substantial amount of Wireless Data.

33. Unauthorized access to Mertz's personal and work-related Wireless Data invades his objectively reasonable expectations of privacy, and invades his rights to privacy.

34. On information and belief, a GSV vehicle has collected, and defendant has stored, and decoded Mertz's Wireless Data on at least one occasion.

CLASS ALLEGATIONS

35. Plaintiff Van Valin brings this action on her own behalf, and on behalf of the following sub-Class:

> All residents within the state of Oregon whose Wireless Data was intercepted, stored, and/or parsed, decoded, or decrypted by defendant.

36. Plaintiff Mertz brings this action on his own behalf, and on behalf of the following sub-Class:

> All residents within the state of Washington whose Wireless Data was intercepted, stored, and/or parsed, decoded, or decrypted by defendant.

37. Excluded from this class are defendant, any person, firm, trust, corporation, officer, director, or other individual or entity in which defendant has a controlling interest or which is related to or affiliated with defendant, and the legal representatives, heirs, successors-in-interest or assigns of any excluded party.

38. Plaintiffs and members of the Class are so numerous that joinder of all members individually, in one action or otherwise, is impractical.

39. This action involves questions of law and fact common to plaintiff Van Valin and all members of the Oregon sub-Class which include:

(a) Whether defendant has engaged in an unlawful invasion of plaintiff's and class members' privacy interests;

(b) The appropriate amount of nominal damages necessary to compensate plaintiff and class members for defendant's invasion of their privacy interests;

(c) The appropriate amount of punitive damages under Oregon law necessary punish defendant for its conduct, and prevent further, similar conduct by defendant and others in the future;

(d) Whether defendant's conduct violated of one or more of the provisions of 18 U.S.C. § 2511;

(e) The appropriate amount of statutory damages necessary to compensate

plaintiff and the class members under 18 U.S.C. § 2520;

(f) The appropriate amount of punitive damages necessary to punish defendant for its conduct, and prevent further, similar conduct, pursuant to 18 U.S.C. § 2520;

(g) The appropriate amount of costs and attorney fees that should be reimbursed or paid to plaintiff and the class under 18 U.S.C. § 2520;

(h) Whether defendant's conduct violated of one or more of the provisions of 47 U.S.C. § 605;

(i) The appropriate amount of statutory damages necessary to compensate plaintiff and class members under 47 U.S.C. § 605 (e)(3);

(j) The appropriate amount of costs and attorney fees that should be reimbursed or paid to plaintiff and the class under 47 U.S.C. § 605 (e)(3);

(k) Whether plaintiff and the class members are entitled to injunctive relief relating to the proper and appropriate time and manner of retention or destruction of the Wireless Data intercepted and stored by defendant and belonging to plaintiff and the class members.

(l) Whether plaintiff and the class members are entitled to injunctive relief enjoining defendant from obtaining any particular class or type of Wireless Data from any wireless network or wireless AP within the state of Oregon.

40. This action involves questions of law and fact common to plaintiff Mertz and all members of the Washington sub-Class which include:

(a) Whether defendant has engaged in an unlawful invasion of plaintiff's and class members' privacy interests;

(b) The appropriate amount of nominal damages necessary to compensate plaintiff and the class members for defendant's invasion of their privacy interests;

(c) Whether defendant's conduct violated R.C.W. 9.73.030;

(d) The appropriate amount of statutory damages necessary to compensate plaintiff and the class members under R.C.W. 9.73.060;

(e) The appropriate amount of costs and attorney fees that should be reimbursed or paid to plaintiff and the class under R.C.W. 9.73.060;

(f) Whether defendant's conduct violated of one or more of the provisions of 18 U.S.C. § 2511;

(g) The appropriate amount of statutory damages necessary to compensate plaintiff and the class members under 18 U.S.C. § 2520;

(h) The appropriate amount of punitive damages necessary to punish defendant for its conduct, and prevent further, similar conduct, pursuant to 18 U.S.C. § 2520;

(i) The appropriate amount of costs and attorney fees that should be reimbursed or paid to plaintiff and the class under 18 U.S.C. § 2520;

(j) Whether defendant's conduct violated of one or more of the provisions of 47 U.S.C. § 605;

(k) The appropriate amount of statutory damages necessary to compensate plaintiff and class members under 47 U.S.C. § 605 (e)(3);

(l) The appropriate amount of costs and attorney fees that should be reimbursed or paid to plaintiff and the class under 47 U.S.C. § 605 (e)(3);

(m) Whether plaintiff and the class members are entitled to injunctive relief relating to the proper and appropriate time and manner of retention or destruction of the Wireless Data intercepted and stored by defendant and belonging to plaintiff and the class members.

(n) Whether plaintiff and the class members are entitled to injunctive relief

enjoining defendant from obtaining any particular class or type of Wireless Data from any wireless network or wireless access point within the state of Oregon.

41. Plaintiff Van Valin's claims are typical of the claims of the members of the Oregon sub-Class, and plaintiff Mertz's claims are typical of the claims of the members of the Washington sub-Class.

42. The named plaintiffs are willing and prepared to serve the Court and proposed sub-Class in a representative capacity with all of the required material obligations and duties. Plaintiffs will fairly and adequately protect the interests of the Class and have no interests adverse to or which directly and irrevocably conflict with the other members of the Class.

43. The self-interests of the named Class representatives are co-extensive with, and not antagonistic to those of the absent Class members. The proposed representative will represent and protect the the interests of the absent Class members.

44. The named plaintiffs have engaged the services of the counsel listed below. Counsel are experienced in litigation, complex litigation, and will protect the rights of and otherwise effectively represent the named Class representatives and absent Class members.

45. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because joinder of all parties is impracticable. The damages suffered by individual class members may be relatively small, the expense and burden of individual litigation makes it inefficient and ineffective for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this case as a class action.

46. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual members, which would establish incompatible standards of conduct for defendant. Defendant has acted on grounds that apply

generally to the Class, making equitable and monetary relief appropriate to the Class as a whole.

FIRST CLAIM FOR RELIEF

(Invasion of Legally Protected Privacy Interests - Oregon Sub-Class)

47. Plaintiff Van Valin realleges paragraphs 1 through 29, 35, 37 through 39, 41 through 46 and further alleges:

48. After collecting, decoding, and/or parsing the data it collected from plaintiff and class members using APs with the unmodified, factory default settings, Google could determine at least the following information: (1) the contents of their personal and private electronic communications; (2) the location or address from where the electronic communication was sent or received; (3) the MAC Address of their wireless AP, which in turn identifies the manufacturer of the wireless AP; (4) the MAC Address, and therefore the manufacturer of at least three other pieces of hardware within their home or facility; (5) their Internet Protocol ("IP") address, which can be used with readily available tools to (a) identify the user's connection method (i.e. DSL, cable, etc.), (b) identify their internet service provider, (c) in some cases identify the user by name and address, and can be used after interception and storage to determine (d) the make and version of the operating system on their computer, and (e) which network server programs they are running on their computer; and (6) the IP address to which internet traffic was directed by them, which can be used to identify the specific website or portal they were visiting at the time of interception.

49. After collecting, decoding, and/or parsing the data it collected from class members using APs with settings modified to encrypt their wireless communications, and from class members using APs with settings modified to both encrypt their wireless communications and hide their SSIDs from discovery, Google could determine at least the following: (1) the contents of their personal and private electronic communications; (2) the location or address from where the

electronic communication was sent or received; (3) the MAC Address of their wireless AP, which in turn identifies the manufacturer of the wireless AP; (4) the MAC Address, and therefore the manufacturer of at least three other pieces of hardware within their home or facility; (5) their Internet Protocol ("IP") address, which can be used with readily available tools to (a) identify the user's connection method (i.e. DSL, cable, etc.), (b) identify their internet service provider, (c) in some cases identify the user by name and address, and can be used after interception and storage to determine (d) the make and version of the operating system on their computer, and (e) which network server programs they are running on their computer; and (6) the IP address to which internet traffic was directed by them, which can be used to identify the specific website or portal they were visiting at the time of interception.

50. The unique MAC Addresses intercepted and stored by Google from all available wireless APs during its GSV process can potentially be used to (a) defeat certain types of security sometimes employed for a user's Wireless APs called MAC Address filtering, (b) "spoof" or copy the user's MAC Address falsely reflecting that it belonged to another piece of hardware to obtain access to restricted internet-based websites and services, and (c) determine whether and where the owner of hardware with that unique MAC Address has accessed another wireless AP.

51. Defendant's conduct was an intentional intrusion upon plaintiff's and class members' private affairs or concerns, and would be offensive to a reasonable person.

52. Defendant's conduct constituted the tort of invasion of privacy with respect to plaintiff and class members.

53. Plaintiff and class members are entitled to nominal damages to compensate for defendant's invasion of their privacy.

54. The Oregon sub-Class in entitled to recover punitive damages in an amount to be

determined by the jury, but sufficient to prevent the same or similar conduct by defendant and others in the future.

SECOND CLAIM FOR RELIEF

(Invasion of Privacy - Washington Sub-Class)

55. Plaintiff Mertz realleges paragraphs 1 through 24, 30 through 34, 36 through 38, 40 through 46, 48 through 50 and further alleges:

56. Defendant's conduct was an intentional intrusion upon plaintiff's and class members' private affairs or concerns, and would be offensive to a reasonable person.

57. Defendant's conduct constituted the tort of invasion of privacy with respect to plaintiff and class members.

58. Plaintiff and class members are entitled to nominal damages to compensate for defendant's invasion of their privacy.

THIRD CLAIM FOR RELIEF

(R.C.W. 9.73.030 - Washington Sub-Class)

59. Plaintiff Mertz realleges paragraphs 1 through 24, 30 through 34, 36 through 38, 40 through 46, 48 through 50 and further alleges:

60. Defendant's conduct with respect to plaintiff and each class member was a violation of R.C.W. 9.73.030.

61. Pursuant to R.C.W. 9.73.060, plaintiff and each class member is entitled to damages and relief as follows:

(a) for plaintiff and each class member, statutory damages of $100 each time that individual's Wireless Data was obtained by defendant, up to a maximum of $1,000 to plaintiff or any individual class member;

(b) reasonable attorneys' fees and other reasonable costs of litigation.

FOURTH CLAIM FOR RELIEF

(18 U.S.C. § 2511)

62. Plaintiffs reallege paragraphs 1 through 46, 48 through 50 and further allege:

63. Defendant's conduct was a violation of 18 U.S.C. § 2511.

64. Pursuant to 18 U.S.C. § 2520, each of the plaintiffs and each class member whose electronic communication was intercepted is entitled to damages and relief as follows:

(a) statutory damages of whichever is the greater of $100 each day that individual's data was obtained by defendant, or $10,000 per violation suffered by that individual;

(b) punitive damages in an amount to be determined by the jury, but sufficient to prevent the same or similar conduct by defendant and others in the future;

(c) reasonable attorneys' fees and other litigation costs reasonably incurred.

SIXTH CLAIM FOR RELIEF

(47 U.S.C. § 605)

65. Plaintiffs reallege paragraphs 1 through 46, 48 through 50 and further allege:

66. The Wireless Data transmitted by plaintiffs and class members constituted interstate communications by wire or radio.

67. Google was not entitled to receive the Wireless Data it intercepted and stored from plaintiffs and class members. After Google received, or assisted in receiving the intercepted Wireless Data, it used the information for its own benefit or for the benefit of another not entitled thereto, in connection with one or more of Google's or its affiliates or licensees' businesses, location based services, and/or as described in part in Google's United States Patent Application No.

12/315,079.

68. Google manufactured, assembled, or modified electronic, mechanical, or other devices or equipment knowing or having reason to know that the devices or equipment were intended for activities prohibited by 47 U.S.C. § 605(a), in violation of 47 U.S.C. § 605(e)(4).

69. Defendant's conduct was willfully committed and for the purposes of direct or indirect commercial advantage or private financial gain. Plaintiffs and class members are, therefore, entitled to an increase of damages to the amount of $100,000 for each violation of 47 U.S.C. § 605.

70. Pursuant to 47 U.S.C. § 605(e), each of the plaintiffs and each class member is entitled to damages and relief as follows:

(a) for each plaintiff and each class member, statutory damages of not less than $1,000 and not more than $10,000 each time that individual's data was obtained or intercepted and stored by defendant. 47 U.S.C. § 605(e)(3)(C)(i)(II);

(b) an increase of statutory damages to up to $100,000 per violation, per individual. 47 U.S.C. § 605(e)(3)(C)(ii);

(c) a reasonable attorneys' fee and other litigation costs reasonably incurred.

REQUEST FOR RELIEF

Plaintiffs request a judgment against defendant and in favor of plaintiffs and class members:

A. Certifying this action as a class action as set forth above;

B. Compensating plaintiffs and all class members with nominal damages for invasion of their privacy interests;

C. Punishing defendant by requiring it to pay punitive damages to Van Valin and the

Oregon sub-class for its intentional invasion of their privacy interests;

D. Compensating plaintiff Mertz and the Washington sub-class member with statutory damages under R.C.W. 9.73.030 equal to $100 for each time any plaintiff's or class member's data was obtained by defendant, up to a maximum of $1,000 damages to each plaintiff or class member;

E. Compensating each plaintiff and class member with statutory damages under 18 U.S.C. § 2520 equal to the greater of $100 for each time any plaintiff's or class member's data was obtained by defendant, or $10,000 per violation suffered by each plaintiff or class member;

F. Punishing defendant for its wrongful conduct by requiring it to pay punitive damages under 18 U.S.C. § 2520 in an amount to be determined by the jury, but sufficient to prevent the same or similar conduct by defendant and others in the future;

G. Compensating plaintiffs and the class members for reasonable attorneys' fees and other litigation costs reasonably incurred in pursuing their remedies under 18 U.S.C. § 2520;

H. Compensating each plaintiff and class member with statutory damages under 47 U.S.C. § 605 of not less than $1,000 and not more than $10,000 for each time defendant intercepted and stored or obtained any plaintiff's or class member's data;

I. Compensating each plaintiff and class member with increased statutory damages of up to $100,000 per individual, pursuant to 47 U.S.C. § 605(e)(3)(C)(ii);

J. Compensating plaintiffs and the class members for reasonable attorneys' fees and other litigation costs reasonably incurred by plaintiffs and the class in pursuing their remedies under 47 U.S.C. § 605.

/ / / / /

/ / / / /

/ / / / /

K. Compensating plaintiffs and the class members for all other costs, relief, and damages legally available under the claims and allegations set forth in this Amended Complaint.

Dated: June 21, 2010.

RICK KLINGBEIL, PC

Rick Klingbeil
OSB #933326
Ph: (503) 473-8565
rick@klingbeil-law.com