CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

NO: 500-06-000567-111

(Class Action)
SUPERIOR COURT

M. ELKOBY

Petitioner

-vs.-

GOOGLE, INC., legal person duly incorporated, having its head office at 1600 Amphitheatre Parkway, City of Mountain View, State of California, 94043, USA

and

GOOGLE CANADA CORPORATION, legal person duly incorporated, having its head office at 1959 Upper Water Street, Suite 900, City of Halifax, Province of Nova Scotia, B3J 2X2

Respondents

MOTION TO AUTHORIZE THE BRINGING OF A CLASS ACTION
&
TO ASCRIBE THE STATUS OF REPRESENTATIVE
(Art. 1002 C.C.P. and following)

TO ONE OF THE HONOURABLE JUSTICES OF THE SUPERIOR COURT, SITTING IN AND FOR THE DISTRICT OF MONTREAL, YOUR PETITIONER STATES AS FOLLOWS:

I. GENERAL PRESENTATION

A) THE ACTION

1. Petitioner wishes to institute a class action on behalf of the following group, of which he is a member, namely:

- all residents in Canada whose electronic data and communications sent or received on wireless internet connections were intercepted by the Respondents' Google Street View vehicles from March 30th 2009 to May 7th 2010, or any other group to be determined by the Court;

Alternately (or as a subclass)

- all residents in Quebec whose electronic data and communications sent or received on wireless internet connections were intercepted by the Respondents' Google Street View vehicles from March 30th 2009 to May 7th 2010, or any other group to be determined by the Court;

2. The present action involves the Respondents intentional [or the very least, grossly negligent] interception and acquisition through Class Members' wireless internet connections "(WiFi connections") of their personal and private information without permission or consent and in violation of their privacy rights;

3. The Respondents also misrepresented the nature of its Google Street View service ("GSV"). While Google told the general public it was collecting and displaying images only, in fact, it was also secretly gathering personal data and information received and sent over privately owned, individual WiFi connections;

B) THE RESPONDENTS

4. Respondent Google, Inc. ("Google USA") is an American company. It is a multinational public cloud computing and internet search technologies corporation. Google USA hosts and develops a number of internet-based services and products;

5. Respondent Google Canada Corporation ("Google Canada") is a subsidiary of Google USA and who does business throughout Canada, including the province of Quebec in the industry of "service d'informatique" and the "exploitation et traitement de données", the whole as appears more fully from a copy the company's *registre des enterprise du Québec*, produced herein as **Exhibit R-1**;

6. Given the close ties between the Respondents and considering the preceding, both Respondents are solidarily liable for the acts and omissions of the other. Unless the context indicates otherwise, both Respondents will be referred to as "Google" for the purposes hereof;

C) THE SITUATION

7. Google Street View ("GSV") is a feature of Google Maps and Google Earth that provides photographic views from various positions along many streets, roads, and pathways throughout the world;

8. Google Street View displays images taken from a fleet of specially adapted cars. On each of these cars there are nine directional cameras for 360° views at a height of about 2.5 meters, GPS units for positioning, and three laser range scanners for the measuring of up to 50 meters 180° in the front of the vehicle;

9. In 2006, Google generated programming code that sampled and decoded all categories of publicly broadcast WiFi 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 particular types of networks, an Ethernet sniffer or wireless sniffer ("wireless sniffer"). As data streams flow across the wireless network, the sniffer secretly captures each packet (or discreet package) of information, then decrypts / decodes and analyzes its content according to the appropriate specifications. Google's software also captured network and router names (commonly called SSID's, an acronym for Service Set Identifier) which is information that uniquely names wireless networks, as well as MAC addresses (Media Access Control) which is a unique identifier assigned to most network adapters or network interface cards. The GSV's data system collected "payload data", specifically 600 gigabytes of information that included emails, videos, audio components, documents, and other personal data sent over the internet such as names, usernames, passwords, phone numbers, email addresses and civic addresses. After Google collected and decoded / decrypted user's payload data, it stored the information on its servers;

10. To view data secretly captured by a wireless sniffer in readable or viewable form, after being captured and stored in digital media, it must then be decoded using crypto-analysis or similar programming or technology. Because the data "as captured" by the wireless sniffer is typically not readable by the public absent sophisticated decoding or processing, it can reasonably be expected and understood to be private, protected information by users and operators of WiFi systems;

11. Users had an expectation of privacy with respect to the payload data collected and decrypted / decoded by Google. Because the GSV packet sniffing data collection was done without the public's knowledge and with software that is essentially undetectable, users could not and did not give their consent to Google's activities;

12. The data collection hardware and software technology that Google developed was approved by before authorizing its inclusion in the Google Street View vehicles and sending them off into the world to obtain information. In fact, Google sought to patent the process. 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 was the assignee of the '776 Application, the whole as appears more fully from a copy of said patent application, produced herein as **Exhibit R-2**. The '776 Application discloses a method devised by Google for gathering, analyzing, and using data sent by users over their wireless routers and other wireless access points (collectively "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."

13. On October 7th 2009, Google released a Press Announcement that Google Street View had come to Canada in which they state:

> "Google has gone to great lengths to ensure Canadians' privacy while enabling them to benefit from Street View on Google Maps."

the whole as appears more fully from a copy of said announcement, produced herein as **Exhibit R-3**;

14. In April 2010, Germany's Federal Commissioner for Data Protection discovered that Google's Street View vehicles were collecting much more than just photographs;

15. In response, on April 27th 2010, Google published on it European Public Policy Blog the following reassurance:

> "What do you mean when you talk about WiFi network information?
>
> WiFi networks broadcast information that identifies the network and how that network operates. That includes SSID sate (i.e. the network name) and MAC address (a unique number given to a device like a WiFi router).
>
> Networks also send information to other computers that are using the network, called payload data, but Google does not collect or store payload data."

the whole as appears more fully from a copy of said blog, produced herein as **Exhibit R-4**;

16. However, on May 17th 2010, Google updated their blog and admitted that they really collect payload data, as they stated:

> "Nine days ago the data protection authority (DPA) in Hamburg, Germany asked to audit the WiFi data that our Street View cars collect for use in location-based products like Google Maps for mobile, which enables people to find local restaurants or get directions. His request prompted us to re-examine everything we have been collecting, and during our review we discovered that a statement made in a blog post on April 27 was incorrect.
>
> In that blog post, and in a technical note sent to data protection authorities the same day, we said that while Google did collect publicly broadcast SSID information (the WiFi network name) and MAC addresses (the unique number given to a device like a WiFi router) using Street View cars, we did not collect payload data (information sent over the network). But it's now clear that we have been mistakenly collecting samples of payload data from open (i.e. non-password-protected) WiFi networks, even though we never used that data in any Google products."

the whole as appears more fully from a copy of said update, produced herein as **Exhibit R-5**;

17. On June 1st 2010, the Office of the Privacy Commissioner of Canada announced that they had launched an investigation into Google's collection of data from unsecured wireless networks as its cars were photographing streetscapes for its Street map services, the whole as appears more fully from said news release, produced herein as **Exhibit R-6**;

18. On October 19th 2010, the Office of the Privacy Commissioner of Canada concluded the following:

> "Google Inc. contravened Canadian privacy law when it inappropriately collected personal information from unsecured wireless networks in neighbourhoods across the country, an investigation has found.
> ...
> The personal information collected included complete e-mails, e-mail addresses, usernames and passwords, names and residential telephone numbers and addresses. Some of the captured information was very sensitive, such as a list that provided the names of people suffering from certain medical conditions, along with their telephone numbers and addresses.
>
> It is likely that thousands of Canadians were affected by the incident."

the whole as appears more fully from said news release, produced herein as **Exhibit R-7**. The full Preliminary Letter of Findings is produced herein as **Exhibit R-8**;

19. On March 21st 2011, the *Commission nationale de l'informatique et des libertés* (“CNIL”) in France fined Google 100,000 Euros for their breach of privacy violations and stated:

> « Dans sa décision du 17 mars 2011, la formation contentieuse de la CNIL relève que GOOGLE a pris l'engagement de cesser la collecte de données Wi-Fi par ses "Google cars" et de supprimer les données de contenu enregistrées selon elle par erreur. En revanche, elle constate qu'elle n'a pas renoncé à utiliser les données identifiant les points d'accès Wi-Fi de particuliers à leur insu. En effet, cette collecte n'est aujourd'hui plus réalisée par les "Google cars", mais s'opère directement par le biais des terminaux mobiles des utilisateurs se connectant au service de géolocalisation Latitude (smartphones, etc.), et ce à leur insu. La CNIL considère que ce défaut d'information constitue une collecte déloyale au sens de la loi, qui était déjà à l'œuvre avec les "Google cars". »

the whole as appears more fully from a copy of said article, produced herein as **Exhibit R-9**;

D) THE FOREIGN PROCEDURES

Several class actions were filed in the United States and consolidated in the Northern District of California, the whole as appears more fully from a copy of said Complaints, produced herein *en liasse* as **Exhibit R-10**. A copy of the Transfer Order MDL No. 2184 is produced herein as **Exhibit R-11**;

II. FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY THE PETITIONER

20. During the class period, Petitioner used and maintained an open wireless internet connection ("WiFi connection") at his home;

21. Petitioner 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, and other personal identification information;

22. Petitioner’s home can be seen on Google Maps and Street View. On information and belief, the Respondents surreptitiously collected, decoded, and stored data from his WiFi connection, including payload data;

23. Petitioner did not know that Google collected his personal information, nor did he give permission for Google to do so;

24. Petitioner has learned of the institution of several class actions filed in the United States and their consolidation regarding the facts as alleged in the present proceedings;

25. Petitioner's damages are a direct and proximate result of the Respondents' conduct;

26. In consequence of the foregoing, Petitioner is justified in claiming damages;

III. FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY EACH OF THE MEMBERS OF THE GROUP

27. Every member of the class used and maintained an open wireless internet connection ("WiFi connection") at his home;

28. Each member of the class has had their privacy rights violated due to the Respondents' unlawful actions;

29. All of the damages to the class members are a direct and proximate result of the Respondents' conduct;

30. In consequence of the foregoing, members of the class are justified in claiming damages;

IV. CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

A) The composition of the class renders the application of articles 59 or 67 C.C.P. difficult or impractical

31. The use of open wireless internet connections are widespread in Quebec and Canada;

32. Petitioner is unaware of the specific number of persons who use open wireless internet connections, however, it is safe to estimate that it is in the tens of thousands (if not hundreds of thousands);

33. Class members are numerous and are scattered across the entire province and country;

34. In addition, given the costs and risks inherent in an action before the courts, many people will hesitate to institute an individual action against the

Respondents. Even if the class members themselves could afford such individual litigation, the court system could not as it would be overloaded. Further, individual litigation of the factual and legal issues raised by the conduct of Respondents would increase delay and expense to all parties and to the court system;

35. Also, a multitude of actions instituted in different jurisdictions, both territorial (different provinces) and judicial districts (same province), risks having contradictory judgements on questions of fact and law that are similar or related to all members of the class;

36. These facts demonstrate that it would be impractical, if not impossible, to contact each and every member of the class to obtain mandates and to join them in one action;

37. In these circumstances, a class action is the only appropriate procedure for all of the members of the class to effectively pursue their respective rights and have access to justice;

B) The questions of fact and law which are identical, similar, or related with respect to each of the class members with regard to the Respondents and that which the Petitioner wishes to have adjudicated upon by this class action

38. Individual questions, if any, pale by comparison to the numerous common questions that predominate;

39. The damages sustained by the class members flow, in each instance, from a common nucleus of operative facts, namely, Respondents' misconduct;

40. The recourses of the members raise identical, similar or related questions of fact or law, namely:

    a) Did the Respondents capture, collect, and/or decode Class Members' payload data, including their personal information, without their knowledge or consent?

    b) Did the Respondents violate Class Members' privacy rights?

    c) Did the Respondents act intentionally, negligently, and/or carelessly when violating Class Members' privacy rights?

    d) What is the appropriate amount of damages necessary to compensate Class Members for the Respondents defendant's invasion of their privacy interests?

e) Are the Respondents liable to pay compensatory, moral, punitive and/or exemplary damages to Class Members, and, if so, in what amount?

41. The interests of justice favour that this motion be granted in accordance with its conclusions;

V. NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

42. The action that the Petitioner wishes to institute on behalf of the members of the class is an action in damages;

43. The conclusions that the Petitioner wishes to introduce by way of a motion to institute proceedings are:

GRANT the class action of the Petitioner and each of the members of the class;

DECLARE the Defendants solidarily liable for the damages suffered by the Petitioner and each of the members of the class;

CONDEMN the Defendants to pay to each member of the class a sum to be determined in compensation of the damages suffered, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay to each of the members of the class, punitive damages, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay interest and additional indemnity on the above sums according to law from the date of service of the motion to authorize a class action;

ORDER the Defendants to deposit in the office of this court the totality of the sums which forms part of the collective recovery, with interest and costs;

ORDER that the claims of individual class members be the object of collective liquidation if the proof permits and alternately, by individual liquidation;

CONDEMN the Defendants to bear the costs of the present action including expert and notice fees;

RENDER any other order that this Honourable court shall determine and that is in the interest of the members of the class;

A) The Petitioner requests that he be attributed the status of representative of the Class

44. Petitioner is a member of the class;

45. Petitioner is ready and available to manage and direct the present action in the interest of the members of the class that they wish to represent and is determined to lead the present dossier until a final resolution of the matter, the whole for the benefit of the class, as well as, to dedicate the time necessary for the present action before the Courts of Quebec and the *Fonds d'aide aux recours collectifs*, as the case may be, and to collaborate with his attorneys;

46. Petitioner has the capacity and interest to fairly and adequately protect and represent the interest of the members of the class;

47. Petitioner has given the mandate to his attorneys to obtain all relevant information with respect to the present action and intends to keep informed of all developments;

48. Petitioner, with the assistance of his attorneys, are ready and available to dedicate the time necessary for this action and to collaborate with other members of the class and to keep them informed;

49. Petitioner is in good faith and has instituted this action for the sole goal of having his rights, as well as the rights of other class members, recognized and protecting so that they may be compensated for the damages that they have suffered as a consequence of the Respondents' conduct;

50. Petitioner understands the nature of the action;

51. Petitioner's interests are not antagonistic to those of other members of the class;

B) The Petitioner suggests that this class action be exercised before the Superior Court of justice in the district of Montreal

52. A great number of the members of the class reside in the judicial district of Montreal and in the appeal district of Montreal;

53. The Petitioner's attorneys practice their profession in the judicial district of Montreal;

54. The present motion is well founded in fact and in law.

FOR THESE REASONS, MAY IT PLEASE THE COURT:

GRANT the present motion;

AUTHORIZE the bringing of a class action in the form of a motion to institute proceedings in damages;

ASCRIBE the Petitioner the status of representative of the persons included in the class herein described as:

- all residents in Canada whose electronic data and communications sent or received on wireless internet connections were intercepted by the Respondents' Google Street View vehicles from March 30th 2009 to May 7th 2010, or any other group to be determined by the Court;

Alternately (or as a subclass)

- all residents in Quebec whose electronic data and communications sent or received on wireless internet connections were intercepted by the Respondents' Google Street View vehicles from March 30th 2009 to May 7th 2010, or any other group to be determined by the Court;

IDENTIFY the principle questions of fact and law to be treated collectively as the following:

a) Did the Respondents capture, collect, and/or decode Class Members' payload data, including their personal information, without their knowledge or consent?

b) Did the Respondents violate Class Members' privacy rights?

c) Did the Respondents act intentionally, negligently, and/or carelessly when violating Class Members' privacy rights?

d) What is the appropriate amount of damages necessary to compensate Class Members for the Respondents defendant's invasion of their privacy interests?

e) Are the Respondents liable to pay compensatory, moral, punitive and/or exemplary damages to Class Members, and, if so, in what amount?

IDENTIFY the conclusions sought by the class action to be instituted as being the following:

GRANT the class action of the Petitioner and each of the members of the class;

DECLARE the Defendants solidarily liable for the damages suffered by the Petitioner and each of the members of the class;

CONDEMN the Defendants to pay to each member of the class a sum to be determined in compensation of the damages suffered, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay to each of the members of the class, punitive damages, and ORDER collective recovery of these sums;

CONDEMN the Defendants to pay interest and additional indemnity on the above sums according to law from the date of service of the motion to authorize a class action;

ORDER the Defendants to deposit in the office of this court the totality of the sums which forms part of the collective recovery, with interest and costs;

ORDER that the claims of individual class members be the object of collective liquidation if the proof permits and alternately, by individual liquidation;

CONDEMN the Defendants to bear the costs of the present action including expert and notice fees;

RENDER any other order that this Honourable court shall determine and that is in the interest of the members of the class;

DECLARE that all members of the class that have not requested their exclusion, be bound by any judgement to be rendered on the class action to be instituted in the manner provided for by the law;

FIX the delay of exclusion at thirty (30) days from the date of the publication of the notice to the members, date upon which the members of the class that have not exercised their means of exclusion will be bound by any judgement to be rendered herein;

ORDER the publication of a notice to the members of the class in accordance with article 1006 C.C.P. within sixty (60) days from the judgement to be rendered herein in LA PRESSE and the NATIONAL POST;

ORDER that said notice be available on the various Respondents' websites with a link stating "Notice to wireless internet connections users";

RENDER any other order that this Honourable court shall determine and that is in the interest of the members of the class;

THE WHOLE with costs including publications fees.

Montreal, April 29, 2011

(S) Jeff Orenstein

_____

CONSUMER LAW GROUP INC.
Per: Me Jeff Orenstein
Attorneys for the Petitioner