

# GOOGLE STREETVIEW NEW ZEALAND PRIVACY IMPACT ASSESSMENT

## August 2011

### I. Project Description

#### A. The Street View Project's Overall Aims

Google Inc. ("Google") has conducted a privacy impact assessment of its Street View project in New Zealand. The goal of the Street View project is to enhance users' experience in Google Maps and Google Earth with 360-degree street-level imagery of public spaces and privately-owned properties that have granted appropriate access to Google. These panoramic images promote greater understanding of a particular location and, among other things, provide useful geographic context. For example, users worldwide have praised Street View for improving driving directions by allowing them to visualize unfamiliar driving routes, before even turning the ignition key in their cars. We believe New Zealand users -- like users around the world -- enjoy the benefits of Street View to help them locate and find more information about local businesses; enrich driving directions; assist in both the sale and purchase of real estate; and promote tourism to New Zealand. At the same time, Google's success depends on the continued trust of its users. In order to earn and maintain such trust, Google takes privacy concerns seriously and the Street View project is no exception.

#### B. The Street View Project's Scope and Extent

Street View imagery and related vehicle positioning (e.g., GPS) data is typically gathered by automobiles driving on New Zealand public roads or, in limited cases, privately-owned locations where Google has received permission to do so in advance. These automobiles use cameras and equipment to capture photographic images and match them to specific geographic locations. Gathered imagery is not posted in real-time. Instead, after collection, the imagery is processed and digitally "sewn" together to create a 360-panorama for users to view and interact with. As part of its continued effort to improve the quality of its mapping services, Google has been gathering and publishing this imagery for countries around the world.

In addition to gathering imagery and data (as further discussed in Section II, "Mapping of Information Flows," below) from cars, Google uses "Trikes" to collect imagery of public places (or in certain instances, privately-owned locales with requisite permission) not readily accessible by automobile. Trikes are tricycles outfitted to carry Street View equipment and capture imagery in areas such as hiking and biking trails. Street View vehicles (i.e., automobiles and Trikes) are operated by third-party contractors trained by Google.

The Street View project is designed to collect information about and facilitate the visualization of places. To the extent images of pedestrians or other individuals may be collected, such collection is purely incidental to Street View's purpose and Google takes a number of steps to protect individual privacy accordingly. As further described below, Google has built and deployed industry-leading tools (such as facial and license plate blurring as well as the "Report a problem" tool) and processes to protect people's privacy.

## C. Links to Existing Programs or Other Projects

### *1. Google Maps API*

In addition to using Street View imagery and information in its own products and services - e.g., Google Maps and Google Earth, Google also offers access to this data to third parties through Google's API feed. This API allows these third parties to add Street View images to their own websites. Importantly, images continue to be controlled, hosted and served by Google through the API, and no imagery is transferred from Google to the third party.

### *2. Discontinuation of Wi-Fi Data Collection*

In May 2010, Google announced that it was voluntarily grounding its Street View fleet and immediately ceasing the collection of Wi-Fi data with Street View vehicles. Prior to resuming Street View driving for imagery and related vehicle positioning data, Google has taken specific and documented steps to terminate all Wi-Fi data collection capabilities on the vehicles. Specifically, Wi-Fi equipment has been removed from New Zealand Street View vehicles and the software will be updated. We will inspect all New Zealand Street View vehicles prior to relaunch. This will be done using a protocol validated by the independent security firm, Stroz Friedman LLP, to ensure WiFi data collection capabilities are terminated.

Google has already updated the vehicle hardware and removed the external USB wireless network adapters and external radio antennas from Street View cars in New Zealand. Because the on-board computers lack built-in wireless network cards, they will not have the physical capability to collect Wi-Fi data without those external USB wireless network adapters and radio antennas.

The updates to the software on the New Zealand Street View vehicles will occur the next time the cars are activated. The software update will remove the following software packages designed to detect, collect and store information from Wi-Fi networks: gslite, gstumbler, Kismet, Wireshark, and tcpdump. As mentioned above, an independent information security firm has reviewed and certified that, after this update, Street View vehicles will have neither the hardware nor the software necessary to detect, collect or store 802.11 wireless network data - including SSIDs (Service Set Identifiers), MAC (Media Access Control) addresses, and payload data. For your convenience, a copy of the independent report is being submitted concurrently with this assessment.

All Street View vehicles in New Zealand will be inspected prior to their re-activation to ensure that the updates have been properly deployed.

## **II. Mapping Information Flows and Privacy Framework**

### A. Information Flows

When the Street View project resumes driving in New Zealand, Google will collect imagery and related vehicle positioning data on public streets and pathways or, in some cases, privately-owned locations where Google has received permission to do so in advance. The following types of data will be collected:

- photographic imagery from digital camera sensors;

- three-dimensional laser scans; and
- telemetry data collected from the following instruments: GPS (Global Positioning System), IMU (Inertial Measurement Unit, to measure movement of the vehicle), and the vehicle's internal CAN (Controller-Area Network, for data such as wheel speed and gear).

### *1. What Information Is Collected*

The primary type of data collected by Street View vehicles consists of digital images of places taken in sequence at spaced intervals. These images are stored in JPEG format along with approximate date and time stamp information. Street View vehicles also collect three-dimensional laser (a.k.a., "point cloud") scans, which help measure the distance from the vehicles to buildings around them and create more accurate mapping. The laser scan data enables users to navigate around the published Street View images. Finally, telemetry data - including GPS, IMU and CAN - is used to improve the accuracy of information regarding a vehicle's location when the images are taken. GPS data regarding a vehicle's geographic location is collected from satellite-based sensors. IMU sensors provide information regarding a vehicle's axis and angular movement, while CAN data provides mechanical readings such as wheel speed. All of this collected information is necessary for Google to provide an accurate and high-quality service for its users.

Given that Street View collects imagery of street-level views, certain images may include people and/or vehicle license plates that are visible in these open spaces. To be clear, Street View has no use for identifiable images of people or license plates, and will not tie such images to information about individuals or their identity. In order to address this incidental collection of information and protect individual privacy, Street View employs a comprehensive approach consisting of proactive steps (including driver training, guidelines on route planning, outreach to certain peak bodies, and automatic blurring of faces and license plates) as well as rich user-facing tools (e.g., the "Report a problem" tool).

### *2. How Information Is Used*

The collected data is used to provide street-level views of locations in certain Google products and services - e.g., Google Maps and Google Earth. Prior to posting images to users, Google will continue its practice of automatically blurring people's faces and license plates. We will also retain un-blurred copies of images to improve Google's blurring technology; extract vital cartographical information; develop innovative and useful new features consistent with Google's Privacy Principles and internal privacy review processes; and ensure the accuracy and quality of Google's mapping products.

For example, objects such as traffic signs, street names and business information are essential for map-making, but are often mistaken by the blurring technology for human faces or license plates, and thus incorrectly blurred. When working to improve the quality of Google's map data, or when a user flags these inaccuracies, Google relies on the original un-blurred images to confirm the information shown on the signs.

Google, however, will permanently blur the original copies of images within twelve (12) months of their posting on Google Maps/Earth.

### 3. Internal Flows

The imagery and vehicle positioning data is initially captured by the equipment and software mounted on the Street View vehicles. The data is written to hard drives located inside the cars and maintained in binary format. The drives are locked with a machine-generated algorithm, and data can only be read by specified Google systems. The drives are physically transferred from New Zealand to the United States of America. Specifically, at the conclusion of each collection activity, the locked hard drives are removed from a vehicle's on-board computer, and transported by a courier to the United States where the drives' data is uploaded onto secure Google servers for processing - *e.g.*, blurring of faces and license plates, and sewing to create a 360-degree panorama. Imagery that is posted on Google Maps or Google Earth is then made available to users worldwide.

During driving, low resolution snapshot sample imagery -- typically not of sufficient quality to identify a person, car or even a house -- is captured at fixed time intervals. These low resolution images, along with other telemetry readings (*e.g.*, GPS coordinates), are transmitted in real-time (via a cellular connection) to Google in the United States, where they are used and stored for sampling and quality control purposes.

### 4. Security Measures

As with all of its services, Google will continue to apply strict data security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data. These measures include periodic internal reviews of Google's data collection, storage and processing practices as well as physical security measures to prevent unauthorized access to Google's systems. While Street View vehicles generally are operated by third-party contractors, as described in subsection 3 above, the collected data is maintained in binary format on hard disks locked with machine-generated keys until it is uploaded to Google's secure servers. The data itself can only be properly read by specified and proprietary Google systems. Furthermore, once uploaded, the data is only accessible to a limited set of authorized Google employees with training on the proper handling of sensitive data. Google's Code of Conduct and internal guidelines establish privacy and security requirements for all employees to follow. Finally, Google is a member of the EU-U.S. Safe Harbor framework, and completes an annual Safe Harbor compliance certification.

### B. Privacy Framework

Google has committed itself to understanding and complying with the laws of each and every country where Street View operates. Each product at Google, including the Street View project, is assigned a product counsel from the Legal Department. The designated product counsel is then responsible for assisting the product team to understand legal issues that may impact a product or service prior to launch, including privacy regulations and laws. In the case of Street View services and operations in New Zealand, the Street View team not only benefited from the involvement of product counsel, but also from the extensive knowledge and advice of Google's privacy law specialists and local lawyers - including external counsel with expertise in New Zealand privacy laws such as the Privacy Act 1993 ("Privacy Act"), its associated privacy principles, and other potentially applicable legal frameworks.

A significant part of Google's comprehensive legal assessment focused on the determination of whether the collection of images from public spaces is prohibited under the Privacy Act. However, this was but a starting point for our analysis. Because we are mindful of the range,

depth and complexity of the laws that may impact Street View, Google not only sought advice on national privacy laws and principles, but also on sensitive locale issues such as airports and military installations. Google carefully considered the legal assessments to assist it in determining an acceptable and appropriate method and management of the Street View collection activities.

While we are not aware of anything in New Zealand law that prohibits the collection of images in public spaces, Google also remains respectful of privacy concerns flowing from the collection and publication of Street View imagery. Therefore Google carefully analyzed and formulated numerous measures - spanning from product development through proposed deployment - to minimize not only legal risks but to address community expectations and concerns in a positive and constructive manner. These steps are discussed in greater detail in the "Privacy Management" section below, and include: training programs for vehicle operators; guidelines to drivers to plan routes in a way that minimizes the possibility of inadvertent collection in prohibited or private areas; advanced automated blurring of human faces and vehicle license plates; effective image flagging, removal tools for users; and submission and review of Privacy Design Documents pertaining to Street View.

### **III. Privacy Impact Analysis**

As part of its impact analysis, Google considered the potential privacy impact of collecting imagery and related vehicle positioning data in public spaces including: (1) images incidentally featuring passers-by and information such as vehicle license plates; (2) images that may trigger privacy-related sensitivities based on the possible association of a person to a particular place; and (3) images that may feature sensitive locales such as women's refuges.

Furthermore, following its announcement that Street View vehicles had mistakenly collected unencrypted WiFi payload data, Google conducted an internal review of its privacy and security practices. Based on this review, Google has made changes to its (1) privacy processes, (2) training programs, and (3) privacy leadership structure.

Google's privacy management framework - as detailed below - addresses the above in a manner consistent with the Privacy Act and its associated guiding principles.

### **IV. Privacy Management**

Google has taken proactive and concrete steps to address privacy concerns prior to and following images being posted on its products such as Google Maps and Google Earth. For Street View in New Zealand, Google has adopted a multi-layered privacy management approach which includes: (1) training of Street View vehicle operators prior to and during collection of imagery as well as guidance on appropriate route planning; (2) disclosure of collection activities; (3) outreach and education to sensitive groups regarding the launch and flagging process; (4) delayed publication of images and automatic blurring of faces and license plates prior to the posting of imagery; and (5) the "Report a problem" tool. These steps are now also complemented by the Google Privacy Assurance Program (detailed below) which covers: (1) Privacy Design Document reviews, (2) training, and (3) privacy leadership across Google's projects and products - including Street View.

## A. Imagery Collection and Publication

Google's privacy management framework for collection and publication of Street View imagery covers the following areas:

### 1. Vehicle Operator Training and Route Planning

Street View vehicles are typically operated by contractors who are regularly trained and reminded of Google's Street View vehicle operation policies. In addition to safety training, operators are trained to only navigate public roads (unless Google has received advance permission to do so in privately owned places), optimize collection to minimize privacy concerns around potentially sensitive locations (such as schools at start and close of the school day, women's refuges, and homeless shelters), and refrain from collecting imagery where it is prohibited to do so.

### 2. Disclosure of Driving Activities

The Street View project strives to be transparent about its collection activities and provides an easily accessible disclosure of where Street View vehicles may be operating and regularly updates this information. By visiting the "Where is Street View?" page on Google's Street View website ([www.google.com/streetview](http://www.google.com/streetview)), individuals can access a drop-down menu and review information regarding where Street View collection activities may be occurring. In addition, Street View vehicles are clearly marked with Google logos.

### 3. Outreach and Education Prior to Posting of Images

As part of the deployment of Street View in New Zealand, Google briefed peak bodies for women's refuges and homeless individuals given the particular sensitivities tied to those groups prior to the posting of imagery to Google Maps and Google Earth. Specifically, Google informed the appropriate peak bodies of the date when Street View imagery would be posted, and educated these bodies about removal tools (further discussed below) which allowed them to review imagery expediently and request an appropriate course of action - *e.g.*, blurring or removal.

### 4. Delayed Publication and Automatic Blurring

Street View images do not identify the owner or occupier of a house, nor are images posted to Google Maps or Google Earth in real-time or available with specific date and time stamps. As such, Street View images do not reflect property ownership or a person's whereabouts at a specific date and time.

In addition, Google uses automated blurring technology to protect individual privacy. This technology detects identifiable faces and legible license plates within images, and blurs those areas prior to the image being posted on Google Maps or Google Earth.

### 5. "Report a problem" Tool

In addition to using its automatic blurring technology, Google offers its intuitive and industry-leading "Report a problem" tool, empowering users to flag imagery for privacy concerns (*e.g.*, further manual blurring of faces - regardless of whether they are or know the individual in question) or inappropriate content (*e.g.*, nudity). Users can also report any image that features

themselves, their family, their car or their home for removal, even if the image has already been blurred.

This tool is accessible through a link at the bottom-left of every Street View image. Individuals simply flag a particular area of an image, and specify the category their concern relates to (e.g., "Privacy Concerns," "Inappropriate Content," etc.). They are then given the option to describe the issue to assist Google's reviewers in processing the request - e.g., "This is a picture of my house" - and asked to provide an email address and complete a CAPTCHA prior to submitting the request. The submitted email address is only used to manage the "Report a problem" process (e.g., spam prevention and status of request updates).

Submitted reports are reviewed and the relevant imagery is further blurred or removed, as appropriate. Information about this process is on the StreetView homepage at [www.google.co.nz/streetview](http://www.google.co.nz/streetview) under the 'Privacy' tab. Individuals who are unable to access to the Internet can write to their local Google office, from where the request is forwarded to Google Inc. in the United States for processing.

## **B. Privacy Assurance Program**

In addition to the above, Google has taken steps to strengthen its overall privacy review process. These additional steps are detailed below:

### **1. Privacy Design Documents**

In late 2010, Google established a policy requiring engineering project leaders to submit, maintain and update Privacy Design Documents for all projects. The Privacy Design Documents require project leaders to describe what user data is being collected as well as how that data is being handled. This requirement applies to projects that: (1) have already been launched, including Street View, (2) have yet to be launched, or (3) may never be launched outside of Google. Members of cross-functional Privacy Review Teams then review and analyze submitted documents for compliance with Google's privacy practices and applicable laws. If necessary, the Privacy Review Teams flag documents for in-depth review, analysis (including for example, code audits to ensure the software behaves as expected), and other follow-up. These teams are comprised not only of experienced privacy and product counsel, but also of engineers and product managers who have demonstrated privacy leadership and knowledge within Google. Furthermore, the completion and submission of design documents will be part of a project leader's regular performance review. Documents pertaining to Street View imagery collections have been submitted and reviewed by a Privacy Review Team.

In addition to the above systematic checks, the Privacy Design Documents will be reviewed by Google's Internal Audit Team which will conduct periodic audits to verify completion of selected documents and the privacy practices of certain products. The Privacy Review Teams will periodically request project leaders to review and update their Privacy Design Document - including during Google's annual review of products for compliance with the U.S.-EU Safe Harbor.

### **2. Privacy Training**

Google is revamping its privacy training programs, and has launched targeted privacy training programs for new hires joining Engineering/Product Management functions. It is also developing

similar programs for employees in the Sales, People Operations, and Legal functions. Furthermore, Google has launched a mandatory data security training module for all Google employees, and will be developing a companion privacy module. Finally, the privacy component of Google's new employee orientation program has been reviewed and updated.

### 3. Privacy Leadership


On October 22, 2010, Google announced the appointment of Alma Whitten as director of privacy across both engineering and product management. Dr. Whitten and her team have been tasked with overseeing privacy processes for engineering and product teams, as well as leading Google's privacy by design efforts. Dr. Whitten's team is also working closely with members from other functions to make sure that all Google employees understand and follow Google's privacy practices and policies.

## **V. Recommendations**

Google will continue to strive to improve quality of its mapping products and make them as user-friendly as possible while remaining conscientious about individuals' privacy concerns. As part of such effort, Google will:

- continue to improve its automatic facial and license plate blurring technology;
- continue to fine tune the "Report a problem" tool based on feedback from users;
- continue to improve its training program for Street View vehicle operators in a manner that is consistent with the privacy-related sensitivities as well as the project's objectives and scope;
- continue to communicate with users about Street View and Street View collection activities - for example, through the Official Google New Zealand Blog (<http://google-newzealand.blogspot.com/>);
- engage with the Office of the Privacy Commissioner regarding material changes to the Street View practices outlined in this PIA; and
- continue to develop and fine-tune its Privacy Assurance Program.





STROZ FRIEDBERG

**Report of Inspection and Remediation  
Of Google Street View Vehicles'  
802.11 Wireless Network Traffic  
Capture Capabilities**

**Submitted By: Eric Friedberg, Jennifer Martin, Jason Novak  
Date: July 20, 2010**

The purpose of this memorandum is to document the inspection of the Google Street View vehicles' hardware and software capabilities conducted by Stroz Friedberg, LLC ("Stroz Friedberg").

Between June 21, 2010, and July 16, 2010, Stroz Friedberg inspected two Google Street View vehicles, a Chevrolet Cobalt and a Subaru Impreza and analyzed the equipment and computers in those cars. The vehicles each contained a computer, a monitor, GPS equipment, CDMA wireless modems, 3-D geometry laser scanners, a camera, and a switch. Both cars were equipped with an antenna built into the car for AM/FM radio, and one was equipped with an antenna for the reception of XM satellite radio. Each vehicle also had the necessary equipment to power the electronic devices enumerated above. It was represented by Google to Stroz Friedberg that the Cobalt was running the production version of the Street View operating system and software, and that the Impreza was running the development version of the Street View operating system and software.

Neither of the vehicles had radios or antennas suitable for the reception or transmission of 802.11 wireless network radio signals. Stroz Friedberg was informed by Google that the vehicles' computers did not have wireless network cards built into them, but rather, had historically been equipped with external USB wireless network adapters. The specific USB wireless network adapters used varied over time; however, we were informed that all USB wireless network adapters previously used were based on the Zydas 1211 chipset and were connected to Maxrad BMMG24005 radio antennas. In both of the cars that we inspected, the USB wireless network adapters and the radio antennas had been removed.

Stroz Friedberg made forensic images of the hard drives in the computers in both cars using I.C.S. ImageMAStter Solo-3 devices, commonly used forensic imaging devices. An inspection of the forensic images was then undertaken to determine what, if any, wireless network detection and or wireless network traffic capture software was present. Stroz Friedberg was informed by Google that the Street View operating system was a customized version of the Ubuntu 8.04 LTS Linux distribution. Review of the forensic images confirmed this.

Stroz Friedberg searched the forensic images for the gstumbler software, for Kismet software, and for other commonly known wireless network detection and traffic capture software. We did so through an inspection of the installed packages, and through keyword searching the names of files on the drives with keywords such as "gslite," "gstumbler," "kismet," and "wireshark," for example.

Stroz Friedberg found that the gslite and Kismet software packages were not present on either of the cars' hard drives. In addition, neither car was equipped with an antenna or wireless adapter suitable for 802.11 wireless data capture.

We did, however, find what appeared to be a number of files that appeared to be remnants that survived the process of Google's initial attempt to remove this software from the hard drives before resuming Street View operations. Among those files detected on both the Cobalt and Impreza hard drives were: a) a small number of shell scripts and configuration files relating to Kismet and Wireshark,<sup>1</sup> b) tcpdump software, a network traffic analysis

<sup>1</sup> These artifacts included: a) a shell script located at /var/lib/dpkg/info/kismet.postrm that removes Kismet log directories when the Kismet package is uninstalled from the computer;

program, and c) the software library libpcap, a software library for the capture and analysis of network packets. However, through an analysis of the forensic images, we determined that the libpcap libraries were installed to support the use of the point-to-point protocol, a protocol used by modems, including cellular modems, to communicate.

We also found, as one would expect in a normal operating system environment a) software to communicate with wireless network adapter hardware devices, and b) software and libraries used by the operating system to configure wireless network cards—including software designed to detect wireless networks and connect a computer to them. These programs are typically installed as part of the operating system installation process, and do not detect wireless networks without the appropriate hardware.

Using the above information, Google personnel wrote a series of remediation scripts to remove the following from the Google Street View computer hard drives: a) the Kismet and Wireshark shell scripts and configuration files; b) all gslite and gstumbler remnants; c) tcpdump; and d) where practicable, software used by the operating system to configure wireless devices. Stroz Friedberg reviewed those scripts and is satisfied from a programming perspective that the scripts will achieve their desired technical objective.

Stroz Friedberg also forensically re-reviewed the Google Street View hard drives of two GSV vehicles, again a Cobalt and an Impreza, after the remediation scripts were run, and determined that the programs did, in fact, remove the files that they were intended to remove. Accordingly, we can and do represent that these two cars have neither hardware nor software capable of capturing or storing 802.11 wireless network traffic. We further represent that if Google applies the remediation scripts to the hard drives in the GSV fleet, and if the cars in those fleets contain (and lack) the same hardware as do the two cars that we inspected, then none of the cars in that fleet should be able to capture or store 802.11 wireless traffic.

---

b) a Lua programming language script designed to enable the use of Wireshark with the Lua programming language; and c) Kismet configuration files.