

Privacy in the Age of Google Street View

Mona Abou Taka

Athabasca University

Author Note

Mona Abou Taka is a Master of Science in Information Systems

Student at Athabasca University, Alberta Canada.

Abstract

Google Street View has emerged on the Internet scene a decade ago and with it rose several privacy concerns voiced by the international community. Albeit the concerns by local communities were vocal and some countries banned the service from taking pictures of its streets, buildings and homes, the global footprint that it has made is phenomenal. However, the negatives seem to outweigh the positives regarding the human right to privacy. Secretly collecting payload data through Wi-Fi, and blurring faces, licence plates numbers and even homes automatically for public consumption does not seem enough to eradicate the privacy concerns from all over the world. It is Google's way of reducing the privacy concerns and several lawsuits, and continue its endeavour of having a massive database of photographed streets and areas for public use in every area of the world.

Keywords: Google, Google Street View, privacy

Privacy in the Age of Google Street View

The recent events of the past decade regarding Google's global scale domination of the public usage of the Internet by mapping streets has sparked an endless debate of human rights privacy violations pretraining to its Google Street View service. From news reports regarding lawsuits concerning privacy breaches, an in-depth analysis of the Wi-Fi "payload data" gathering from 2007 to 2010 without warning to the public that such maneuver was taking place, to Google's automated solution of blurring faces, licence plates, and upon request, homes too to reduce the privacy concerns. This paper examines the privacy concerns and breaches of the service and compares them to positive results that Google is trying to achieve at the expense of human's right to privacy.

Literature Review

News agencies have been reporting on law suits and accusations of Google Street View's service, especially the "payload data" from unencrypted Wi-Fi networks that they have been storing. Per Burdon et al. (2013), "GPS signals and satellites are extremely accurate, but Wi-Fi mapping is more beneficial because it is energy efficient and reliable indoors where satellite accessibility is restricted (p. 703). Therefore, Google has been collecting Wi-Fi data because location-based service relies on header data from Wi-Fi access points such as residential and business modems and routers to offer interactive location and mapping application (p. 702). Yet, Google secretly collected Wi-Fi unencrypted header data from the years 2007 to 2010. A news article from eWeek.com claimed that Google has also captured entire emails, whole password and other identifying private information from opened unencrypted Wi-Fi access points. "Google said in May [2010] that Street View, a Google Maps feature that records images of city streets all over the world, had accidentally stored 600 gigabytes of citizen's data from more than

30 countries since 2007” (Google Street View Captured Whole Passwords, 2010). Also, the news article states that Google is taking the matter seriously and it is training its 23,000 employees the new security awareness program because the mistaken act was getting a rise out of privacy advocates who have vilified the company over the “WiSpy” issue.

Although the claim of Google’s unawareness of the data collected has emerged again on April 30, 2012 per eWeek.com news outlet by reporting that Google’s staff knew that the street cars were collecting private data. The street cars are “normal cars on top of which are mounted panoramic cameras developed by Google and based on the open hardware camera, Elphel. These cars drive through the streets by day during good weather, automatically taking panoramic views every 10–12 metres from a height of 3–4 metres” (Hoelzl et al., 2014, p. 262). Google goes through great plains to collect images from its Street View cameras, and it has run afoul of privacy laws in many countries. An investigation by the Federal Communications Commission (FCC) found that an engineer told two other colleagues in 2007 that personal data including Internet usage histories was being collected with other Wi-Fi information (Google Staff Knew, 2012). After thorough investigation by the FCC, Google has admitted that for the first time that the engineer’s software was deliberately written to capture payload data, and that data could be useful to Google in other programs other than Street View. With this incident, “Google came under harsh criticism from consumer privacy advocates and regulators in both the United States and Europe in 2010 after it was learned that between 2007 and 2010, the Street View vehicles had collected the payload data” (Google Staff Knew, 2012). The privacy violations that stemmed from Google’s act of storing the payload data has been reported on March 14, 2013, and it settled privacy infringements with authorities in 38 U.S. states with a record payment of \$7 million U.S. in the process (Google's Street View: Cars, cameras, 2013).

The stored payload data that was a mistake until Google admitted its true intentions and payed for it spurred further privacy concerns with its automated blurring of moving subjects in captured photos. The automated blurs are a filter where images are passed through it where faces, licence plates and other potentially identifying information are blurred. However, the filter algorithm sometimes fails; these instances called ‘false negatives’ are ‘food’ for a multitude of blogs and continue to circulate on the web (Hoelzl et al., 2014). Moreover, as Google Street View expands into more “exotic places, it appears to have a problem in many of the towns and cities where the service has been available for years” (Miners, 2015, p. 46) and resulting in gaps that Google claims it as a bug or “known issue” in their software. It refused to answer questions that addresses it may be privacy requests. Although privacy requests are very common, Google verbally fought for it publicly, and as its ex-CEO and now executive chairman Eric Schmidt said in an interview with CNBC (2009), ‘If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place. If you want your building to be blurred in GSV, is it because you have something to hide?’ (Hoelzl et al., 2014).

Discussion

The roll out of Google Street View has spurred a multitude of privacy concerns, many nations voiced their opinions, and some banned the service from its streets. Although Google has made it clear that taking photos from public domains is legitimate, many privacy advocates disagree, and news reports discussing types of data collected say otherwise.

Positive versus Negatives Viewpoints of the Service

Every technology advancement has seen positives and negatives of its usage, and Google services are no different. However, the negative effect concerning privacy breaches in certain

countries and the type of data collected are more vocally discussed than the positive aspects that certain companies are ecstatic about regarding the free public service.

International concerns. The United Nation's ("UN") global coordination and international recognition of human rights began with the Charter of the UN that offers the advancement of human rights. Although the Charter does not explicitly define the human rights that member states are committed to uphold, the UN assembly adopted the Universal Declaration of Human Rights ("UDHR"). Since the UDHR lacked binding authority, it led to the creation of the International Covenant on Civil and Political Rights ("ICCPR") that is signed and ratified by 160 states. Both the UDHR and ICCPR list privacy as a human right (Rakower, 2011, p. 320-321). Despite the widespread recognition of this privacy right protecting it has become an elusive task because of the advanced technologies, and Google Street View service raises complicated questions. "... [I]t not only implicates the privacy rights and protections afforded domestically, but triggers the attention of the entire international community" (Rakower, 2011, p. 322).

Moreover, Google Street View has sparked a profusion of controversy regarding the meaning and functionality of global privacy, and many individuals have been caught in compromising situations resulting in many questions facing the worldwide community regarding the right to privacy and online image management (Rakower, 2011, p. 325). Some of these compromising situations are: naked female in Taiwan, dead bodies in Brazil, and man entering adult video store in the United Kingdom. Furthermore, some countries banned the service completely from its jurisdictions such as Czech Republic, and others like Germany after a long feud with the service where many people objected to it, allowed it to only take images of its big cities like Berlin and Frankfurt (Miners, 2015, p. 49). "Australia joined the ranks of states

conducting investigations that question the legality of Google Street View, and Greece cited privacy reasons for banning Street View within its borders” (Rakower, 2011, p. 327).

Wi-Fi data collection. As mentioned earlier, Google Street View was storing unencrypted Wi-Fi data or “payload data” to aide in location mapping. However, unsecured data from open Wi-Fi networks such as emails, passwords and other private personal information were also stored. Google has “collected MAC addresses, SSID, transmission rate data and location data during the Street View collection exercise. Google contended that the data was not personal information and therefore information privacy law did not apply” (Burdon et al., 2013, p. 715). They were also correct in saying that the default SSID and MAC addresses are unique device identifiers and should not be classified as personal information (p. 715). Yet, this masking of Google’s true intentions became clear; they were caught and admitted the action was purposely done to enhance its other services with such data resulting in an uproar by privacy advocates from all over the world.

Street view public photos for researchers’ advantages. All the negative vocal uproar from Google Street View service has outweighed the positives that was intended to achieve. The public knows that the true intention of the service is mapping world streets to help them visit their intended location and explore other potential areas. In addition, certain researchers in the U.S. use the collected images from Google Street View to offer a promising alternative to “measure neighborhood environments across cities and to examine how neighborhood conditions vary across a wider geographic scope” (Bader et al., 2017, p.18). Although the major concern of privacy arises with the service, it is more difficult to study specific locations without seriously considering the confidentiality of the data (p. 36). There is a risk to pay of using the service and

Google may change its privacy policy at any time, but it helps these researchers reduce massive costs to conduct their studies.

Conclusion

Google Street View has captured images from 7 continents and became an essential online public service that came into existence in the year 2007. With it came a slue of privacy concerns and violations to human rights that the UN and other governing bodies tried to protect for its citizens, but some cases such as the payload data that Google Street View stored from 2007 to 2010 has jeopardised its online presence and positive intentions. Although countries fought the privacy violations, Google continues to make its case of publicly displaying street images, homes and buildings online with blurring faces and licence plates automatically to reduce privacy concerns and continue its online endeavour.

References

- Bader, M. M., Mooney, S. J., Bennett, B., & Rundle, A. G. (2017). The Promise, Practicalities, and Perils of Virtually Auditing Neighborhoods Using Google Street View. *Annals Of The American Academy Of Political & Social Science*, 669(1), 18.
doi:10.1177/0002716216681488
- BURDON, M., & McKILLOP, A. (2013). THE GOOGLE STREET VIEW WI-FI SCANDAL AND ITS REPERCUSSIONS FOR PRIVACY REGULATION. *Monash University Law Review*, 39(3), 702-738.
- Google Staff Knew Street View Cars Were Collecting Private Data FCC 276221. (2012, April 30). *eWeek*.
Retrieved from <http://0-go.galegroup.com.aupac.lib.athabascau.ca/ps/i.do?p=AONE&sw=w&u=atha49011&v=2.1&it=r&id=GALE%7CA288215914&asid=fb0f3c6e1306681b74d4c2e21b0cba2a>
- Google Street View Captured Whole Passwords EMails URLs 480162. (2010, October 23). *eWeek*. Retrieved from <http://0-go.galegroup.com.aupac.lib.athabascau.ca/ps/i.do?p=AONE&sw=w&u=atha49011&v=2.1&it=r&id=GALE%7CA240218193&asid=2fbb7f691621a9099aedc239eb86b180>
- Google's Street View: Cars, cameras - and privacy complications. (2013, March 14). *Globe & Mail* [Toronto, Canada], p. B7. Retrieved from
[com/ps/i.do?p=CPI&sw=w&u=atha49011&v=2.1&it=r&id=GALE%7CA322246904&asid=5f1cfb4fb453a9d41388a12c5017cad4](http://0-go.galegroup.com.aupac.lib.athabascau.ca/ps/i.do?p=CPI&sw=w&u=atha49011&v=2.1&it=r&id=GALE%7CA322246904&asid=5f1cfb4fb453a9d41388a12c5017cad4)
- Hoelzl, I., & Marie, R. (2014). Google Street View: navigating the operative image. *Visual Studies*, 29(3), 261-271. doi:10.1080/1472586X.2014.941559

MINERS, Z. (2015). The vanishing: What happened to Google Street View's missing streets?.

Pcworld, 33(8), 46-50.

Rakower, L. H. (2011). BLURRED LINE: ZOOMING IN ON GOOGLE STREET VIEW AND

THE GLOBAL RIGHT TO PRIVACY. *Brooklyn Journal Of International Law*, 37(1),

317-347.

Presentation

The presentation link is found here: <https://landing.athabascau.ca/file/view/2395405/privacy-in-the-age-of-google-street-view>