

UK ICO Finds Google UK Guilty Of Drive-By Snooping, But Imposes No Fine

On November 3, 2010, the UK Information Commissioner issued a press release announcing the result of the Information Commissioner's Office ("ICO") investigation into alleged privacy breaches by Google UK.¹

The ICO investigation followed the revelation that Google's Street View vehicles had inadvertently collected personal information from private internet connections.² Whilst acknowledging that Google's conduct amounted to a breach of the Data Protection Act 1998, the Commissioner decided against the imposition of a fine.

Background to the Breach

Google's Street View facility provides 360-degree photographs of numerous public locations across the globe. In addition to taking these photographs, it has become apparent that Google's fleet of Street View vehicles were also engaged in the mapping of WiFi connections. Through on-board GPS technology, the Google vehicles were able to store the co-ordinates of the wireless networks they drove past on their extensive journeys.

WiFi mapping is not uncommon. By having a record of the GPS co-ordinates of known networks, smartphone users are able to triangulate their approximate location based on nearby wireless connections. Indeed, the improvement of Google's location-based services, of which a number use this location technology, was the reason given by the company to explain why its Street View vehicles were collecting WiFi data.³

Accordingly, whilst WiFi mapping may not be objectionable in itself, opposition surrounds the particular way by which Google conducted its Street View connection-mapping exercise. In addition to collecting the basic information necessary to identify the networks they drove past (such as the names/"SSIDs" of the networks), for the brief time that they were connected to them, the Street View vehicles also collected the data in transit from the networks.

This transit data, known as "payload" data, serves no traditional purpose for WiFi mapping. Indeed, the data is usually encrypted through users' network security measures. Interestingly, the Street View vehicles dropped encrypted payload data, but did not drop the payload data received from the unencrypted connections they drove past. The technology used by Google collected and stored the unencrypted data.

¹ Information Commissioner's Office, *Information Commissioner announces outcome of Google Street View investigation* (Press Release, November 3, 2010) available at http://www.ico.gov.uk/~media/documents/pressreleases/2010/google_inc_street_view_press_release_03112010.ashx

² *Official Google Blog*, May 14 2010, available at <http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html>

³ *Ibid*

The practice came to light in May 2010 following an investigation by German authorities, which sparked investigations around the world in the other countries mapped by Street View. When confronted, Google admitted the practice, but asserted that it was a mistake – blaming the breach on the inadvertent inclusion of an experimental piece of code previously developed by one of Google’s engineers.

Further concern arose following a subsequent Canadian investigation, opened in June 2010. Whilst payload data is largely fragmentary in nature, the Canadian data protection authority discovered that complete e-mails, URLs and passwords could still be identified from the unencrypted payload data stored by Google.

UK Response

Google’s admission prompted further investigation by the UK’s ICO, the results of which have now been announced by the Information Commissioner in a press release dated November 3, 2010. While the Commissioner believes Google’s payload collection practice to have amounted to a “significant” breach of the Data Protection Act 1998, in a move that has surprised many, no monetary penalty has been imposed. The Commissioner has instead insisted that Google UK sign and undertake, requiring the company to improve its data compliance and to submit a compliance audit by the ICO.

On November 19, 2010, the ICO issued a subsequent press release announcing that Google Inc. had signed a commitment to improve its data handling “to ensure breaches like the collection of WiFi payload data by Google Street View vehicles do not occur again”.

Google signed an undertaking committing the company to implementing improved training measures on security awareness and data protection issues for all employees, the ICO said. Google also said it will require its engineers to maintain a privacy design document for every new project before it is launched. Significantly, Google agreed to delete the payload data that it inadvertently collected in the United Kingdom. The ICO added that it will conduct “a full audit of Google’s internal privacy structure, privacy training programs and its system of privacy reviews for new products”.

As the majority of Google’s Street View operations in the United Kingdom were carried out prior to the introduction of the ICO’s fining powers in April 2010, it had been a moot point whether the ICO would have been able to impose a fine.⁴ However, this has largely been cleared up by the recent November 3 press release in which the Commissioner expressly states that, after consideration of the breach, he rejects calls for the imposition of a monetary penalty, and instead views a written undertaking as the most appropriate regulatory action in the circumstances.⁵

The decision not to issue a monetary penalty has attracted criticism from numerous parties, including MP Robert Halfon, who has described the ICO’s decision as “lamentable and lily-livered”. On the other hand, there are those who believe that the uncertainties and complexities surrounding the exact circumstances of the breach in this case would have left the imposition of a fine vulnerable to legal challenge – and

⁴ Josh Halliday, “Google Street View: information commissioner shackled by Data Protection Act” (*Guardian.co.uk*, October 28, 2010) available at <http://www.guardian.co.uk/technology/2010/oct/28/google-street-view-information-commissioner>.

⁵ Note 1 above.

any lengthy legal action could have a considerable impact on the resources of the ICO.⁶

The International Response

The previously noted, Google Street View has mapped numerous countries across the globe. As a result, Google's collection of payload data has been the subject of investigation in 20 separate countries to date – with many investigations still ongoing. While the investigations have largely involved the same objectionable conduct, the responses from the relevant authorities have indeed been varied.⁷

The authorities in Denmark, Austria and Ireland, for example, closed their investigation, merely requiring Google to delete the payload data collected by their vehicles. Google has so far avoided the imposition of a monetary penalty, although many investigations are still to be concluded. Indeed, this run may be about to be coming to an end for Google, as it looks increasingly likely that Spain will be the first country to impose a financial penalty for the data collection.⁸

In the United States, the Federal Trade Commission ("FTC") – in a move similar to that taken by the ICO in the United Kingdom – closed its inquiry into Street View in October 2010, receiving assurances from Google that it would not utilise the payload data and that privacy protections would be improved.⁹

While this perceived lack of action angered many privacy advocates, Google's conduct may still be punished in the United States. Indeed, two weeks after FTC closed its investigation, the Federal Communications Commission announced its ongoing investigation into whether Google's collection of WiFi data contravened the U.S. Communications Act. In addition to federal action, privacy lawsuits have also been brought against Google in over 35 states.

A somewhat interesting development has been the recent call by a watchdog group, the National Legal and Policy Center, for an investigation to be carried out by the House of Representatives Oversight Committee, to look into the relationship between Google and the current U.S. administration, and, in particular, whether the perceived closeness of this relationship played any role in the FTC closing its investigation into Google without imposing any penalty.¹⁰

⁶ "Commissioner plays poker with Google" (*The Register*, November 10, 2010) available at http://www.theregister.co.uk/2010/11/10/commissioner_gives_google_21_days_to_sign_public_undertaking/.

⁷ See further, Josh Halliday, "Google Street View, the investigations around the world" (*Guardian.co.uk*, November 12, 2010) available at <http://www.guardian.co.uk/technology/blog/2010/nov/12/google-street-view-privacy-worldwide>

⁸ Mikael Ricknas, "Spain Moves to Fine Google over Street View" (*Yahoo News*, October 19, 2010) available at http://news.yahoo.com/s/pcworld/20101019/tc_pcworld/spainmovestofinegoogleoverstreetview and Thomas Delclos, "Espana expedienta a Google" (*El Pais.com*, October 19, 2010) available at http://www.elpais.com/articulo/Pantallas/Espana/expedienta/Google/elpepirtv/20101019elpepirtv_1/Tes

⁹ Federal Trade Commission letter available at <http://www.ftc.gov/os/closings/101027googleletter.pdf>

¹⁰ Sara Jerome, "Watchdog wants probe of Google's 'unusually close' ties to Obama" (*The Hill*, November 9, 2010) available at <http://thehill.com/blogs/hillicon-valley/technology/128455-google-clout-with-obama-administration-deserves-an-investigation-watchdog-says>

Conclusion

The Google Street View saga is particularly interesting one. As new technologies are introduced to meet society's ever-increasing demand for information, it becomes more challenging to reconcile this seemingly insatiable appetite for information with expectations of privacy. The current situation highlights that, while this is a challenging dichotomy, the two are not mutually exclusive – improvements can be made on both sides.

This case highlights that an early consideration of the privacy implications of new technologies is paramount in order for innovators to avoid potential problems and maintain their goodwill – a subject matter close to most if not all privacy advocates around the world.

At the same time, the circumstances of the Street View data breach shows that, while companies are ultimately responsible for the privacy implications of their technologies, a better understanding of data security and protection (such as network encryption) can nonetheless afford users optimum protection.

This article featured in the November 2010 issue of World Data Protection Report.

Valerie Surgenor is a Senior Associate with MacRoberts LLP, Glasgow. E-mail: valerie.surgenor@macroberts.com

[See our website for full Copyright notice and Disclaimer.](#)

© MacRoberts LLP 2010