TMT Practice Group

BCCC Attorneys LLC is an independent business law firm with offices in Geneva and Lausanne and clients throughout Switzerland. We have been active in Technology, Media and Telecoms (TMT) for many years and have acquired a strong expertise on cutting-edge legal issues and a deep knowledge of the key industries.

BCCC's TMT practice group key contacts:


MICHEL JACCARD


MANUEL BIANCHI DELLA PORTA


PHILIPPE GILLIERON


VINCENT ROBERT

For more information related to the TMT practice group at BCCC, please visit our website at http://www.bccc.ch.

LEGAL UPDATE RELATED TO GOOGLE'S COLLECTION OF PRIVATE DATA SENT OVER UNSECURED WIRELESS NETWORKS IN PEOPLE'S HOMES.

Background

Google has been the subject of much concern by data protection authorities in Europe over the last year. Such has in particular been the case of Google Street View, which resulted in numerous claims and protests not only in Switzerland, where a case filed to the Administrative Supreme Court is pending[1], but also in Germany[2] and Greece[3].

Since last week, Google however has had to face another blow that could substantially damage its reputation. After having been requested by German data protection to disclose exactly what WiFi data Google's Street View cars collect for location-based products such as Google Maps for mobile, and assured that such data were limited to the publicly broadcast ID number of the WiFi router (so-called MAC address) and the name assigned to it by the owner (so-called SSID), Google had to admit that its data collection performed by roving Street View vehicles was far more extensive and extended to a record of sites viewed by users and potentially the

[1] See http://www.edoeb.admin.ch/themen/00794/01124/01595/index.html?lang=de.
[2] http://www.dw-world.de/dw/article/0,,5222701,00.html.
[3] http://edition.cnn.com/2009/WORLD/europe/05/13/greece.google.street.view.blocked/index.html.

content of messages if users did not secure their WLANs with a password. This disclosure has already been heavily discussed in online news[4] and in the blogosphere[5].

Google immediately acknowledged the problem and provided best efforts to mitigate its damage reputation by recognizing its mistake, stated that such data had never been used and would immediately be deleted, asked a third party to review the software at issue and confirm that data had been deleted appropriately, and internally reviewed its procedures to ensure that its controls are sufficiently robust to address these kinds of problems in the future[6]. So far, an independent third party has already confirmed the deletion of all data identified as originating from Ireland[7].

In spite of such efforts, Google may find it hard to recover the trust of officials. Canadian privacy commissioner Jennifer Stoddard has expressed her concern about the situation, and the US Federal Trade Commission is currently reviewing a letter from advocacy group Consumer Watchdog calling for a federal probe of Google's data harvesting practices[8].

Google may also find it hard to find a way out of the intricacies between data protection and communication regulations. While the company had been ordered by German officials to send over the data it had collected from WiFi networks within a certain deadline, it did not comply and instead requested for additional time to investigate whether such a delivery could amount to a breach of communication regulations. While some privacy campaigners such as the EFF side with Google on this, the company nevertheless could face a fine of several hundreds of thousands of Euros for having missed the deadline[9]. Google is likely to face similar dilemma in others jurisdictions. This has already proved to be the case in Oregon. Following a class action lawsuit filed by citizens who claim their privacy was violated by Google's collection of data from their unsecured home WiFi networks, a federal judge issued a restraining order last week, barring the Internet firm from destroying data and ordering it to turn over two copies of the hard drive containing the data collected[10].

Comment

---

[4] See, among numerous others : http://www.nytimes.com/2010/05/16/technology/16google.html; http://www.ft.com/cms/s/2/254ff5b6-61e2-11df-998c-00144feab49a.html; http://content.usatoday.com/communities/technologylive/post/2010/05/protests-widen-over-googles-global-wi-fi-data-harvesting/1.

[5] See among others : http://www.wi-ficars.com/an-indignant-germany-google%E2%80%99s-%E2%80%98unintentional%E2%80%99-data-harvest/;

[6] http://googleblog.blogspot.com/ of May 14, 2010, updated on May 17, 2010.

[7] http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en//press/pdf/ISEC_Letter.pdf.

[8] http://content.usatoday.com/communities/technologylive/post/2010/05/protests-widen-over-googles-global-wi-fi-data-harvesting/1. For the letter of Consumer Watchdog, see : http://www.consumerwatchdog.org/corporateering/articles/?storyId=34304.

[9] http://www.ft.com/cms/s/f3d42fee-698d-11df-8ae3-00144feab49a,Authorised=false.html?_i_location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2Ff3d42fee-698d-11df-8ae3-00144feab49a.html&_i_referer=.

[10] http://techdailydose.nationaljournal.com/2010/05/judge-bars-google-from-destroy.php.

While there has not been any official press release or public announcement from Hanspeter Thür, the Swiss Data Protection Commissioner, so far, the Swiss Data Protection Authority is likely to put this new blow for Google under scrutiny.

Legally speaking, there is indeed little doubt that the data collected would fall under the Swiss Data Protection Act (DPA) and do not comply with the requirements defined under its Art. 4, i.e.:

- The principle of legality, which prohibits any unfair or deceitful data collection, including hidden collection.
- The principle of good faith, which requires the concerned individuals to have been informed of the collection, the type of data collected as well as the purpose and length of this collection.
- The principle of proportionality, which only entitles the collection of data that are necessary to achieve the goal sought for. One may doubt that this criterion had been respected here.
- The principle of finality, which only entitles the data collected to be used in the manner disclosed to the concerned individuals.

Arguably, data collected such as content of messages could easily lead to the building of users' profiles, whose treatment is bound to additional requirements (such as informed consent, security measures and declaration of file to the Swiss Data Protection Commissioner).

While all these requirements appear to be burdensome for any companies in the digital age, they should not be neglected. This is all the more true than the concerned company may then have to face a difficult appraisal of the legal situation, as it will have to deal on the one side with an official order requesting the disclosure of the information and on the other side with the secrecy of telecommunications and the very limited circumstances as well as formal requirements under which this secrecy may be waived under Swiss Law.

One should indeed not consider Google an exceptional case. Any high-tech company should draw lessons from this event and implement robust compliance procedures to ensure that their IT infrastructure and software shall not expose it to liability. In a time when privacy is highly valued by citizens and customers, one should not be surprised to have a Court consider a lack of due diligence or implementation of robust procedures to ensure users' privacy and legal compliance as a fault, no matter how costly such an IT audit is, with potentially severe financial consequences not to mention the damage reputation suffered which might be hard to recover.

Contacts: Michel Jaccard, jaccard@bccc.ch | Manuel Bianchi della Porta, bianchi@bccc.ch | Philippe Gilliéron, gillieron@bccc.ch | Vincent Robert, robert@bccc.ch