Cloud data makes life easier for government spooks – and the law gives them a free pass

September 16 2014, by Bill Buchanan

Our digital footprints will prove much more enduring. Credit: Tamas Kovacs/EPA

With the growth of internet-based cloud services, storage, social media and mobile devices, our activities increasingly leave digital shadows in our wake – social media activity, website visits, mobile phone records – that are hard to escape from.

There have never been so many opportunities for governments around the world to snoop on citizens as there are today. Yahoo recently

released a cache of documents revealing how in 2007 it refused a demand from the US National Security Agency for a bulk release of email metadata. Yahoo fought the demand in the courts, but caved in the following year after it was threatened with fines of US$250,000 a day for refusing to comply.

In the years since Yahoo has fought through the courts to unseal the case documents, in doing so shining a light on the government's data collection activities. The Foreign Intelligence Surveillance Court, which hears requests for information from agencies such as the NSA, has approved almost every request it has received. While huge firms such as Yahoo have been criticised for releasing their users' data, in fact they have doggedly fought against doing so. In this case, Yahoo fought back on Fourth Amendment grounds, which prohibits unreasonable searches and seizures and requires that they be based on probable cause and sanctioned by a judicial warrant. They argued the warrants were too broad in their scope – and thus unconstitutional.

Long arm of the law

While laws such as UK's Data Protection Act exist to prevent misuse of personal information, the sheer volume of data and the ease of access to it provides greater opportunities for snooping. And for every Data Protection Act is a law such as the Regulation of Investigatory Powers Act (RIPA), a UK law passed in 2000 that granted powers of surveillance to a wide range of public bodies, from national security agencies such as MI5 and MI6, to local councils, hospital trusts, even the Post Office. Among these powers is the ability to demand internet and telecommunications records – websites, emails, call and text records.

In the US, the PRISM surveillance program provides an even easier means to access personal information held in the cloud – and this has been used on nine of the largest internet companies, including Microsoft,

Google, Yahoo, Facebook and Apple.

The internet, an (almost) borderless place

One of investigators' greatest challenges is working across national boundaries and UK police often struggle to access data held in cloud infrastructures based in the US. On the other hand, US government agencies seem to have far fewer problems, for example in forcing Microsoft to release information from its Microsoft 365 cloud-based office application service, despite being based in Ireland, not the US.

Google transparency disclosure, 2013

Type	Requests ▲	% Requests accepted	User accounts affected
Subpoena	7,044	84	11,999
Search warrant	2,537	81	4,180
Other court orders	689	75	1,588
Emergency disclosures	153	78	217
Pen register order	140	90	259
Wiretap Order	11	100	11

US government requests for data Google

Under RIPA, UK police and other investigators can access personal data with the support of a warrant, whereas in the US the Patriot Act provides far greater scope if deemed relevant to counter-terrorism or counter-intelligence investigations. At its most extreme, Section 215 of the Act provides US authorities with the right to send National Security Letters to require access to personal data stored in the EU by US-based companies, completely disregarding EU or member state national data protection legislation.

Google's 2013 transparency report revealed it received 53,356 requests for data affecting 85,148 accounts, of which between 75-100% were accepted. For the same year, Microsoft received a total of 35,083 requests related to 58,676 user accounts, with a rejection rate of just 3.4%.

Protecting data

Cloud users should always encrypt sensitive data, but can still be compelled by law to hand over their encryption keys. Christopher Wilson was jailed for six months this year for refusing to decrypt data wanted by Northumbria Police in its investigation into attacks on the force's website. Similarly in 2012, Syed Hussain and three other men were jailed for planning an attack on a Territorial Army headquarters using a home-made bomb mounted on a remotely-controlled toy car. Hussain, who admitted having terrorist sympathies, was handed an additional four months for refusing to provide a password for an encrypted USB stick.

UK citizens have the right to silence, while those in the US have similar rights under the Fifth Amendment. But in both cases an exception exists for encryption keys and – just as with a refusal to answer police questions – the failure to provide encryption keys can be seen as a sign someone has something to hide.

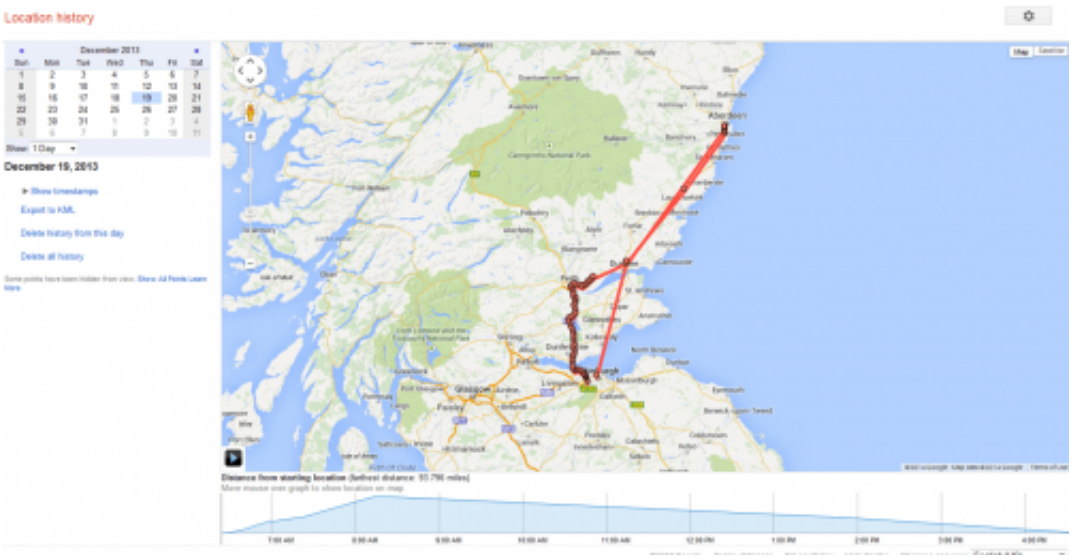
So as the big nine cough up details under PRISM pressure, concern over the scope of government surveillance is increasing. In the US, the Electronic Frontier Foundation award organisations that require a warrant, tell users about government data requests, publish transparency reports, provide guidelines for law enforcement and fight for user privacy rights in the courts and in Congress.

Dropbox, Google, Microsoft, Twitter and Yahoo meet all six of these

conditions, while Amazon meets two (requiring a warrant and lobbying Congress) as does AT&T (publishing reports and guidelines). The Foundation is lobbying Congress to change the law to make it clear that digital information and data is personal property, and should be treated accordingly.

Under the digital shadow

The digital shadow of our online life is continually logged and recorded, reflecting information we provide willingly and also that we release without knowing or outside our control. For example, the Google Cloud contains information on our location, web history, and the apps we use – taken together this can build up a detailed picture of our activities.



From Edinburgh to Aberdeen, as seen by the spy in the cloud. Credit: Bill Buchanan, Author provided

Here is a recent trip I made from Edinburgh to Aberdeen to give a lecture, as recorded by location tracking in an Android phone. Both Apple and Android phones, by default, record and store this information and can store it in the cloud, offering up a goldmine of information to investigators.

As the devices and programs we use become increasingly cloud-based, it's extremely difficult to remove all traces of this digital shadow, especially with back-up systems storing files even after their deletion. Our digital shadow is getting longer, and it is stored largely by US companies. With the demands of PRISM and the Patriot Act, even in the face of European privacy safeguards, these companies have and will give up that information when the spooks come knocking.

Source: The Conversation