National security vs. online privacy

November 7 2014, by Peter Gill

Credit: Negative Space from Pexels

One method for safeguarding online anonymity is Tor, "the onion router", whose name comes from its method of adding and stripping away encryption layer by layer as messages pass from one node to another in the network en route to their destination.

This image of peeling back layers could equally describe the task of trying to establish whether intelligence agencies comply with the law. This is an onion that is, a few layers down under its outer shell, giving off a distinctly mouldy smell.

Any government intrusion into citizens' lives that breaches their human rights should be proportionate – and only made when necessary to safeguard national security or public safety. In the days before the internet this was relatively easy to regulate. Post and telephone calls could only be intercepted in the UK on the basis of a warrant signed by a minister, or in some countries a judge. But the digitisation of practically everything has transformed this process, with the opportunity to "just collect everything" quite possible if the agencies have the will and resources to do so.

The tranche of documents released to the media by whistleblower Edward Snowden has demonstrated the extent to which that will exists.

We knew that material could be obtained from ISPs, telephone companies or the postal service under powers granted by the Regulation of Investigatory Powers Act 2000 (RIPA). We did not know that intelligence agencies also obtain this data by directly tapping the fibre optic cables or the servers and networking equipment at exchanges and data centres – done apparently without the companies' knowledge.

We do not pay for the services we use every day – Google, Facebook, Microsoft, YouTube – except with our personal information. But whether or not we "volunteer" this information knowingly to companies, this does not imply our consent to it being routinely available to governments.

The rapid growth of social media brings into sharp relief concerns about the misuse of personal data. A TNS poll in the UK found that 55% were

concerned about the activities of search engines such as Google, 60% were concerned about social media such as Facebook and 43% were equally concerned about intelligence agency monitoring. And rightly so, it seems.

The Snowden files also give us insight into the collaboration between national intelligence agencies, especially between the five Anglophone nations within the UKUSA agreement from 1946, the formal basis for co-operation that began in World War II and continues into the present.

It has long been suspected that this co-operation was a way in which country A could get around legal restrictions on information gathering at home by receiving the information it sought from the foreign intelligence service of country B.

After the release of the Snowden papers, the parliamentary Intelligence and Security Committee (ISC), a key part of the oversight and regulation apparatus of British intelligence, issued a statement that the allegations GCHQ had illegally accessed material gathered by the NSA were unfounded. Its claim that in every case there was a ministerial warrant failed to reassure anyone outside government, however, and the ISC eventually announced that they would inquire more widely into the issues of privacy and security raised by these revelations.

These are the claims that have now come back to haunt the government, after Liberty and Privacy International challenged the legality of GCHQ's interception practices before the Investigative Powers Tribunal, which hears complaints about improper use of RIPA to conduct surveillance.

Instead, the documents now revealed in court have exposed how false the ISC's statement in response to the Snowden files was. In fact GCHQ can and does request and receive raw unanalysed bulk data from NSA, and

others, with no warrant required if it were not feasible to obtain one in the UK.

This is not surprising to people who study international intelligence co-operation given the complexity – and secrecy – of the arrangements in place. However, this slow striptease of information indicates how inadequate the current law and system of oversight and accountability is. The senior judge with responsibility to oversee interception under RIPA describes the Act as "difficult for anyone to get their head round" and notes that "a reader's eyes glaze over before reaching the end of Section 1, that is, if the reader ever starts."

Bringing about better, clearer laws and more robust oversight of the intelligence agencies will be considerably more difficult and cutting into this mouldy onion will be enough to induce tears.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation