PHYS.ORG

Why Reset the Net falls short in protecting you from surveillance

June 13 2014, by Ashlin Lee

How many ways are you being watched? Credit: GlebStock

A year on from Edward Snowden's revelations around state sponsored mass surveillance programs, some of the major players in the online and technological world (including Google, Mozilla, Twitter and Reddit) have launched the Reset the Net campaign.

The program aims to increase people's awareness and uptake of privacy and security tools so they can better resist surveillance, particularly that conducted by the National Security Agency (NSA).

While the campaign is laudable in its efforts to raise the issue of surveillance, there are some glaring oversights present.

A step in the right direction

Reset the Net seeks to challenge mass surveillance and help people to take back their privacy while online by encouraging patterns of behaviour that resist surveillance.

For individual users they suggest the use of apps with encrypted communications protocols (such as TOR or Chat Secure), and safer password choices.

More structural suggestions are provided for developers and administrators, such as the use of encryption as a part of a website or application, and the use of end-to-end encryption.

Encryption makes any collected data more difficult (but not impossible) for authorities to interpret and act upon.

These kinds of strategies do a great job at "target hardening" users and digital services against the collection of personal data, and they improve the general security of users online.

Vodafone announced this month that some governments allow their security agencies to connect directly into its network to conduct surveillance, so these kind of user based forms of resistance are a good starting point to counteracting some surveillance measures.

While these are positive achievements, they merely address some of the more visible consequences and implications of surveillance, and fail to address what are perhaps the most worrying aspects of contemporary surveillance.

Where the problems lie

The Reset the Net project acts to reinforce the idea that surveillance is primarily conducted by state authorities, with the NSA as the primary antagonist for this story.

But the reality is that the NSA is only one actor in the surveillance drama. As others have noted one of Reset's biggest backers, Google, is also one of the biggest instigators of corporate surveillance.

Google collects enormous amounts of personal data every day, harvesting personal data from user's browsing habits and email, while simultaneously calling for email to be encrypted against outside sources.

Google also uses its large range of products (such as Gmail and Google Docs) to data-mine every conceivable audience, including up until recently children.

You are being monitored by many

Google is just one of many private companies conducting surveillance today, with supermarkets, insurance companies and many Fortune 1000 companies all monitoring customers on a daily basis.

This leads to the next issue with Reset the Net, and most counter-surveillance activities today: they don't address the incredible amounts of data already circulating in surveillance databases.

Surveillance today is not just about seeing into the lives of the present – it's about cataloguing and using the past (and present) to understand the future. Australia is no exception to this trend, as the government once again pushes for mandatory data retention.

As a part of the (so-called) development of big data, which allegedly can assist to generate new statistical insights from ultra-large data sets, the data collected from ubiquitous surveillance are increasingly being used as a part of predictive analytics.

Through these techniques a user's future behaviours, actions and dispositions can be extrapolated from past data. While there are some possible positives here (such as better management of goods and services for business), the negative potentials are enormous.

Shaping the future

The use of algorithms and automated profiles can open the door to forms of control (and discrimination) that occur without any human input.

Through the power of code, corporate or government powerbrokers can reshape individual lives, automatically analysing and predicting possible outcomes for citizens and then determining their treatment, from seemingly random pieces of personal information.

As US sociologist Gary Marx has pointed out, no-one is innocent under such regimes of "new" surveillance, with all citizens viewed as a risk - what he calls categorical suspicion.

The focus on internet surveillance ignores that surveillance is not just on the internet, but everywhere. As recently pointed out, we live in a Sensor Society, with many aspects of daily life recorded through various sensor technologies.

From smartphones to drones, there are many possibilities for invasive surveillance today. The German newspaper Der Speigel has also pointed out that the NSA and Central Intelligence Agency (CIA) are at the forefront of developing new means of sensing individuals.

Once again Google is a part of these trends, recently purchasing a drone company and is reported to be bidding for the world's largest home surveillance company.

The drama is just beginning

Internet surveillance is only one aspect of contemporary surveillance.

The Reset the Net project paradoxically represents a small positive step in resisting and counteracting warrantless and illegal surveillance, while ignoring the bigger picture.

There is a growing and ongoing disparity between the rights and powers of the watched (or sensed), and the watchers (or sensors). As both spectators and actors in this surveillance (or sensor) society, there is a need to be mindful of this bigger picture as we play our roles and choose our props, and recite (or improvise) our lines.

These are only the opening scenes of a much longer and difficult play. With no sign that the social or technological scope of surveillance will fade, we must play our parts wisely and critically, if we are to have any hope of a happy ending.

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

Provided by The Conversation

Citation: Why Reset the Net falls short in protecting you from surveillance (2014, June 13) retrieved 23 June 2024 from https://phys.org/news/2014-06-reset-net-falls-short-surveillance.html