Beyond Privacy: The Cost and Consequences of Mass Surveillance

Esther Kersley

4 September 2015

This week the new UN privacy chief said UK surveillance was "worse than [George Orwell's novel] 1984". In the two years since the Snowden leaks revealed the existence of bulk internet and phone surveillance by US intelligence services and their partners, including the UK, the British government continues to engage in the mass collection of citizens' communications data.

Whilst the US Congress barred the National Security Agency (NSA) from collecting US phone data in bulk in June this year after the US court of appeals ruled it to be unlawful, in the UK the mass collection of communications data was found by both the parliamentary Intelligence and Security Committee and

Latest

An Update on the Security Policy Change Programme

Chances for Peace in the Third Decade

A Story of ORG: Oliver Ramsbotham

David Anderson QC, who is responsible for reviewing UK terrorism legislation, to be legal and should be maintained. Furthermore, the Investigatory Powers Bill, dubbed the "Snooper's Charter", which was blocked by the Liberal Democrats party three years ago, has re-emerged under the Conservative majority government. Now firmly back on the agenda, it would move to strengthen the security services' powers for the bulk interception of communications data.

To date, the debate around mass communications surveillance has focused primarily on the infringement of privacy it entails. But, beyond privacy implications, government mass surveillance programmes come at further costs.

Proliferation, public trust and internet security

A major concern with the development of mass surveillance tools is that they can be used by authoritarian regimes to suppress freedom of information and expression and track down political opponents. There is evidence that this is already happening: Privacy International's publicly available database on the private surveillance sector has found that surveillance companies are selling powerful and invasive surveillance technologies, with the potential for the mass interception of communications, to a number of authoritarian regimes globally, including Bahrain, Ethiopia, Libya and Pakistan. Much of this technology is at pace with the capabilities of the NSA and its UK equivalent, GCHQ, which is having clearly visible consequences. In Ethiopia, for example, mass surveillance technology was found to be used to regularly arrest and detain citizens, in particular as a tool to silence dissenting voices, targeting the ethnic Oromo population. The widespread use of torture and other ill-treatment against political detainees in Ethiopian detention centre makes the use of these technologies even more troubling.

A Story of ORG: Gabrielle Rifkind

Most read

The Role of Youth in Peacebuilding: Challenges and Opportunities

Making Bad Economies: The Poverty of Mexican Drug Cartels

ORG's Vision

Remote Warfare: Lessons Learned from Contemporary Theatres

Another cost of mass surveillance is the weakening of public trust in national governments. An erosion of public trust in government in general (see this report from President Obama's own Review Group on Intelligence and Communications), coupled with a weakening of trust in governments for citizens online security in particular, was found to have occurred since the Snowden leaks. The steep increase in the use of Tor (an open source network that allows users to obscure their online activity) which went from 500,000 daily users worldwide to more than 4 million following the Snowden leaks, as well as an increase in other internet privacy platforms since the leaks seem to confirm this.

Furthermore, the weakening of internet security is another cost of mass surveillance programmes. These programmes rely on creating and maintaining vulnerabilities in communications networks that undermine the communications infrastructures that we all rely on (see this report from The Council of Europe). The creation of "back doors", for example, along with other weaknesses in security standards and implementation could easily be exploited by non-state groups.

In May this year, a group of tech companies, including Facebook, Google and Yahoo (as well as civil society groups and academics) signed a letter to President Obama urging him to oppose efforts that would force companies to build in ways for law enforcement to access products and services protected by encryption. The letter warned that introducing intentional vulnerabilities into secure products for the government's use will make those products "less secure against other attackers", including street and computer criminals, repressive or dangerous regimes and foreign intelligence agencies.

Is mass surveillance stopping terror attacks?

Beyond the risk of proliferation, the weakening of government trust and the threat to internet security, the UK government's reliance on mass surveillance could also come at a cost to its citizens' physical security. The use of data-mining and automated data-analysis techniques used to filter down the vast amounts of data acquired in mass surveillance programmes comes with a high risk of false positives. It has been suggested that data-mining for counter-terrorism in particular comes with a higher risk of false positives than when used in other settings (such as credit card fraud detection) due to the quality of data available and the rarity of terror attacks. This high number of false positives associated with counter-terrorism will, in turn, cause an overload of data, swamping analysts and thus taking resources and attention away from more appropriate counter-terrorism methods.[1]

Recent evidence suggests that mass surveillance may not be an effective tool for foiling terror plots. A number of reports from the US, including a declassified 2009 report from the US government and a report from a review group appointed by President Obama, have shed doubt on the supposed effectiveness of mass surveillance programmes. One in particular, from Washington based think-tank New America Foundation, found traditional investigative methods played a far greater role than mass surveillance in initiating investigations into the majority of terror cases reviewed. In one case (a 2009 plot to attack the Danish newspaper Jyllands-Posten), the US government was found to have exaggerated the role mass surveillance played in thwarting the plot.

Recent terror attacks have further exposed the limits of surveillance. In the Boston Marathon bombing in 2013, for example, it was revealed that the failure to foil the bomb plot was due to a failure in sharing and coordination of

information between departments, rather than the bombers being unknown to intelligence agencies prior to the attack. Similarly, the 2014 Charlie Hebdo and French grocery store attackers in Paris were not only known to French and US authorities but one had a prior terrorism conviction and another was monitored for years by French authorities. In both cases the attackers were known to authorities and had been under surveillance.

Security by 'remote control'

The use of mass surveillance programmes by government must not be seen in isolation but should be viewed as part of the trend towards maintaining security by 'remote control', the global shift towards countering threats at a distance without the need to deploy large military force. As technological advances have increased governments' digital intelligence gathering capabilities, mass surveillance techniques demonstrate the interdependence between intelligence and surveillance and the growing relationship between intelligence, technology and modern combat.

Like the use of drones, special forces and private military companies, the secretive nature of mass surveillance programmes means they operate in an accountability vacuum, with little transparency or oversight, rendering the public unable not only to hold government to account, but to assess these techniques' perceived effectiveness. In the UK, recent Anderson, ISC and RUSI reports all stressed the need for greater transparency and oversight with regards to government mass surveillance programmes.

Like other remote control methods, mass surveillance of citizens' communications data is appealing as it is perceived as cost-free and plays to

Western states' technological strengths. The perceived ease of remote control has, however, blinded policy makers from considering its broader and long term implications. There is a need for greater transparency and accountability with regards to government mass surveillance in the UK, along with a robust regulatory framework for private security companies which are trading surveillance technologies globally. As well as this, far more consideration must be given to the unforeseen and long-term costs of mass surveillance in order to evaluate its utility for long-term sustainable peace and security.

Image Credit: https://pixabay.com/en/camera-cameras-traffic-watching-19223/

The Remote Control project recently published a briefing paper *"Mass surveillance: security by 'remote control' – consequences and effectiveness*", read it here.

[1] For more information please see report by the Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council, "Protecting Individual Privacy in the Struggle Against Terrorists: A framework for program assessment", William Binney in "NSA Struggles to Make Sense of Flood of Surveillance Data", Wall Street Journal, December 2015 http://www.wsj.com/articles/SB10001424052702304202204579252022823658850, and Bruce Schneier, "Why Mass Surveillance Can't, Won't, And Never Has Stopped A Terrorist", digg, March 2015 http://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist

---

Esther Kersley is the Research and Communications Officer for the Remote Control project. Prior to joining ORG, Esther worked in Berlin for the anti-corruption NGO Transparency International as an editorial and online communications officer. She has a particular interest in counter-terrorism and conflict resolution in the Middle East, having previously worked with the Quilliam Foundation and IPCRI (Israel/Palestine Center for Research and Information), a Jerusalem based think tank.

Share this page

Contact

Unit 503
101 Clerkenwell Road London
EC1R 5BX
Charity no. 299436
Company no. 2260840

Email us

020 3559 6745

Follow us

Registered with FUNDRAISING REGULATOR

Useful links

Login
Contact us
Sitemap
Accessibility
Terms & Conditions
Privacy policy