Mass surveillance: my part in the reform of GCHQ and UK intelligence gathering

The GCHQ building in in Cheltenham. 'Take the recent case of Amnesty International's emails being found on GCHQ computers. Does it matter whether or not they were actually read by a person?' Photograph: Barry Batchelor/PA

t was an unusual group. An investigative journalist, a moral philosopher, an internet entrepreneur, a cyber-law academic, a government historian, a computer scientist, a technology exec, a long-time cop, an ex-minister and three former heads of intelligence agencies. I wondered not just how but if we could agree on anything, let alone an entire set of recommendations to reform UK communications surveillance.

Yet we did. The Royal United Services Institute panel was set up by Nick Clegg[1], the then deputy prime minister, in response to revelations from the US whistleblower Edward Snowden[2] about the scale of intrusion by US and British intelligence agencies into private lives. Our remit: to look at the legality, effectiveness and privacy implications of government surveillance; how it might be reformed; and how intelligence gathering could maintain its capabilities in the digital age.

Edward Snowden's revelations made it clear: security oversight must be fit for the internet age

Nick Clegg

Read more

It wasn't easy and there were several times when I thought I would be writing a minority report with one or two of the panel members. But in the end we reached consensus: the report – published today – proposes that the security services continue with bulk collection of communications data, but with improved oversight and safeguards.

It wasn't the ideal any of us individually might have chosen, but neither does it contain items any of us heartily oppose. For me there were four main victories and one loss. At what point is privacy engaged? For the security services and government it only becomes an issue at the point when a human looks at material. This is how vast quantities of data could be intercepted, stored and analysed by computer without much considering of privacy implications. For me privacy is engaged from the moment information is accessed and stored. Take the recent case of Amnesty International's emails being found on GCHQ computers[3]. Does it matter whether or not they were actually read by a person? The mere fact they were intercepted and stored by an intelligence agency is worrying enough.

In bulk collection the potential exists for anyone to be watched at any time. One of the red herrings put our way was that GCHQ does not conduct mass surveillance because it does not read everyone's email. What was not mentioned is that GCHQ[4] might intercept and store large quantities of it, as the Amnesty case demonstrates.

> *For me privacy is engaged from the moment information is accessed and stored*

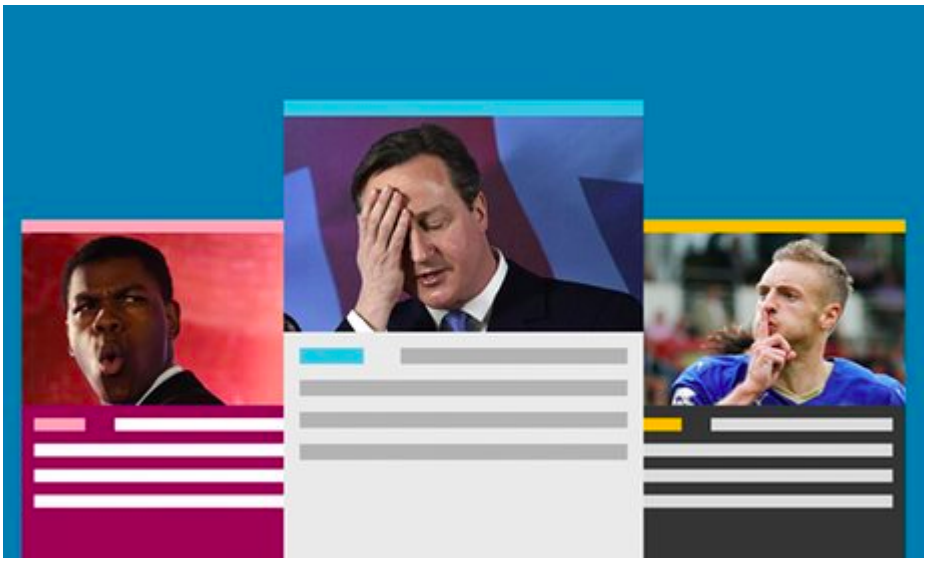
The point of Jeremy Bentham's Panopticon[5] wasn't that everyone was actually watched at all times, it was that they could all potentially be watched. It is the possibility of omnipotent surveillance that acts as a chilling effect on any behaviour that potentially offends the state or the powers that be. For those who commit acts of journalism or legal advocacy that directly challenge state power, the risks in such a society are great.

This is why the report states that privacy is engaged at point of collection and recommends regular review of data retention policies by oversight bodies to ensure they remain proportionate.

Another partial win is changing the way surveillance is authorised. I went on to the panel with a clear goal to shift the system away from authorisation of surveillance by politicians to a more independent judicial system. Most democratic countries abolished political warrants for the reason that political

expediency should not override the constraints of the law. And judicial warrants are more likely to gain cooperation from US internet companies. After all, the US stopped letting politicians sign off intrusive warrants in 1789 with the fourth amendment[6].

The spies and politicians initially wanted no change to the current regime. However the recommendation by David Anderson QC on judicial warrants[7] made it much harder to stick with the status quo. Even so, the majority of panellists opted for a compromise: a largely judicial authorisation system but with the secretary of state signing warrants for national security and economic wellbeing, but subject to judicial review.



The third point may seem innocuous: a recommendation that the commissioners be given a statutory right to refer cases to the investigatory powers tribunal[8]. The IPT is the only "court" where people can seek legal redress against improper surveillance. Yet obtaining evidence to bring a case to court is almost impossible. Groups such as Privacy International, Liberty and Amnesty are reliant on either a whistleblower like Snowden or pure speculative guesswork. The commissioners are the only outsiders allowed to see the inner workings of intelligence gatherers, yet they face prohibitions on disclosure so cannot bring the fullness of their findings into the public domain, nor refer them to the IPT.

Finally, there is a subtle shift away from the "clean bill of health" given to past and current surveillance practices. This was very contested. A good deal of assumptions were made that, in my view, gave the benefit of the doubt to those whom we were supposed to be investigating. The intelligence and security committee report[9] gives conclusive assurances that nothing the intelligence agencies have done is illegal or wrong.

> *Not surprisingly, I encountered most resistance when pushing for information about what the agencies are actually doing*

I, and one or two others, did not feel we had seen enough evidence or knew enough about the activities to give such an assurance. How can we endorse what has not been avowed? The activities we did know about may not be technically illegal (though it is a question still before the courts), but they were done without public knowledge or a public mandate. To use such vast and intrusive powers without a public mandate is more worthy of sanction than endorsement in my opinion. At the very least, past activities show a clear failure to respect the democratic process.

Not surprisingly, I encountered most resistance when pushing for detailed information about what the agencies are actually doing. Are they using personal data from other parts of the government such as the NHS to build algorithms to predict future criminals? I don't know. But if we are to be an informed citizenry – a prerequisite in a democracy – we need the agencies to avow their most intrusive un-targeted surveillance practices. Otherwise, they do not have a public mandate for them. In effect, they are acting outside the democratic system.

It was also impossible to make judgments about the effectiveness of bulk surveillance techniques because the underlying data is available only to those with a stake in promoting its effectiveness, rather like granting a pharmaceutical company with a drug to sell total secrecy over its clinical trials. The best we could do was this: "It is unrealistic for the intelligence agencies and some specialist parts of the police service to operate in very transparent ways. They could not be effective if they did. They should, however, be rigorously and independently held accountable, and the oversight mechanisms must themselves be highly transparent to the public."

Heather Brooke, a professor of journalism, was a member of the RUSI independent surveillance review panel

This article was amended on 14 July 2015. An earlier version said David Anderson's report gave conclusive assurances that nothing the intelligence

agencies had done was illegal or wrong. That is not the case.

1. http://www.theguardian.com/commentisfree/2014/mar/03/nick-clegg-snowden-security-oversight-internet-age
2. http://www.theguardian.com/us-news/edward-snowden
3. http://www.theguardian.com/uk-news/2015/jul/01/gchq-spied-amnesty-international-tribunal-email
4. http://www.theguardian.com/uk/gchq
5. http://www.theguardian.com/commentisfree/2007/feb/12/theparentalpanopticon
6. https://www.theguardian.com/technology/2012/aug/27/twitter-judge-occupy-order
7. http://www.theguardian.com/world/2015/jun/11/uk-intelligence-agencies-should-keep-mass-surveillance-powers-report-gchq
8. http://www.theguardian.com/politics/2014/mar/05/independence-ipt-court-mi5-mi6-home-office-secrecy-clegg-miliband
9. http://www.theguardian.com/us-news/2015/mar/12/intelligence-agencies-finally-understand-need-to-step-out-of-the-shadows