Questions for Parliament: Open Rights Group briefing

Westminster Hall debate on oversight of surveillance

1 Is the oversight working? Was RIPA's warrant system really designed for mass data sweeps? Who holds the Foreign Secretary to account?

These are basic questions about the institutions that oversee surveillance. For instance, the Regulation of Investigatory Powers Act (RIPA) was not designed for mass collection of Internet data, but for small targeted investigations.

It is not clear who knew about what powers GCHQ and the NSA have, even within the National Security Committee of Cabinet. Chris Huhne says he was not informed, for instance.

A number of civil liberties groups have made the following suggestions for areas to reform oversight and transparency (https://www.openrightsgroup.org/ourwork/reports/mass-surveillance-oversight-debate):

1. Commission independent, post-legislative scrutiny of the Regulation of Investigative Powers Act 2000 and the Intelligence Services Act 1994, legislation that covers much internet surveillance but was written years before Facebook existed and when few households had internet access. If Parliament intends to allow the collection of data from every internet communication, it should expressly say so in primary legislation, covering both metadata and content
2. Publish, as the US Government has done, legal opinions that are used to underpin the ongoing surveillance framework
3. Allow the Intelligence and Security Committee to report to Parliament, and be chaired by an opposition MP, as called for by Lord King. It should also be able to employ technical experts to assist its work.
4. Publish the budget and investigatory capacity of the ISC, Interception of Communications Commissioner and Surveillance Commissioners
5. Reform the Investigatory Powers Tribunal so there is a presumption its hearings are held publicly, that it should state reasons for reaching its decisions and that its judgements can be appealed in court
6. End the need for Secretaries of State to approve appearances of the heads of agencies before Parliamentary committees, and allow agency and service heads to give evidence in public where appropriate
7. Establish an independent body to review the work of the agencies, as President Obama has done with the Privacy and Civil Liberties Oversight Board, and ensure it has staff with relevant technical expertise
8. Lift any legal restrictions on British companies from publishing transparency reports about surveillance requests
9. Publish details of the use of surveillance powers broken down by agency, as opposed to the single UK figure currently published, including the scale of international intelligence sharing
10. Enhance whistleblower protection for those who wish to come forward from within the services

2 Do the oversight bodies understand the implications of the technology, and are they capable of

standing up to the security services when they ask for unreasonable powers?

The Internet is a huge change in the way we communicate. Vast volumes of information are generated by every citizen. This is a honey pot for surveillance. There is a massive risk of overbearing state surveillance as information can be gathered from so many places, and is of so many kinds – opinions, contacts, locations.

Understanding the range of risks and what society can tolerate is not a matter of oversight, but democratic debate. Oversight cannot hope to make a strategic balance, rather it seeks to look at a decision to to see if that decision is reasonable within the powers a body has already been granted.

Thus the broad outline of security programmes must be discussed in public.

3 What does "metadata" reveal and is it really safe to collect?

Metadata is the main kind of information collected by the UK's Tempora. Tempora removes content information after three days and retains metadata for 30 days. Metadata includes location, who talks to who, and allows the details of an individual's life to be reconstructed. To assemble this information without Internet and telephone data would require intense directed surveillance. In a sense, therefore, metadata collection and analysis is more powerful than employing directed surveillance on every UK citizen. It is more powerful because data analytics can analyse the results much more intrusively than merely looking at a list of data events.

4 Do programmes need to be secret?

This is a key argument, and the government needs to justify why programmes were kept secret, and whether they understood the risk in doing so.

A common argument is made that 'programmes must be secret' in order that terrorists do not evade the techniques employed. However, details of programmes do tend to leak out to those who are watching. NSA data collection, access at private companies, even GCHQ's taps on cables, were known about, or rumoured, and reported in reputable publications. They did not become the subject of public debate, but criminals would have been able to understand the risks.

On a broader level, Internet technologies are well enough understood to know what intelligence agencies are likely to be doing.

Thus the idea that a data collection programme like Tempora, or access to private data through PRISM, can realistically or needs to remain secret seems like an exaggeration.

On the other side, keeping the operations secret ran a number of risks, firstly that when they were revealed, public confidence in our institutions and businesses working with them would be severely undermined. Secondly, given the international nature of the UK and US data sweeps, they have put at risk our relations with neighbouring states and the citizens of those governments.

Individual investigations of course must remain secret.

5 Do we have enough data to understand what the security services are doing?

Simply, no. We are denied the data we need as a matter of national security.

6 Is it really true that just because your data is examined by a machine, you are not under surveillance?

While an individual's data may not be looked at by a human, it is patently the case that it may be, and the individual is not in control of when that may be. It is hard to argue that is not surveillance.

7 Do we know who is affected by mass surveillance?

It is unclear how abuses are found, recorded and dealt with in the UK. However, evidence from the USA given to Congress shows both common abuses such as checking the records of wives and partners, and a lack of systematic detection, as abuses were usually detected by confession, such as when an agent retired, or gossiped with a colleague, or through the target also at the NSA suspecting

that the abuser had obtained information.

But these are trivial examples compared with the risks to people who routinely need confidentiality, which at some level is all of us. Nor does the US data detail any oversteps that were sanctioned by their authorities.

8 Do we understand the risks that we are putting citizens at?

One programme stands out as a pervasive and unpoliceable risk to citizens – the programmes aimed to break or weaken encrypted communications.

Operations Edgehill (UK) and Bullrun (US) are designed to 'get around' Internet security to enable taps and surveillance, for instance by making it possible to break encrypted content, or get into a program like Skype to listen to a conversation.

However, such vulnerabilities can be used by third parties, and a whole class of software engineers specialise in finding such vulnerabilities. These are known sometimes as 'hackers' or 'crackers', depending on whether they work for security companies to close the loopholes, or criminals to exploit them.

9 Do we understand the business and economic risks?

There are a number of risks to businesses:

- Encryption vulnerabilities, that could be exploited by criminals, resulting from Operation Bullrun and Edgehill.
- Commercial confidentiality risks for businesses competing with the USA, as information can be exploited by US intelligence. US intelligence activities have an economic remit. PRISM and Tempora both place UK businesses at risk
- Lack of trust and decline in customer usage, particularly in relation to the US cloud. UK customers and businesses may not wish to gain the benefits of US cloud services because of the risks of access to private data through PRISM.
- Lack of confidence in UK and US security products, as a result of Operations Bullrun and Edgehill – any UK security product is potentially compromised

10 Do we understand the risks to our democracy?

Many of the risks we are running are about the power of the state to abuse democratic rights, such as the ability to use information against common or garden protesters, to investigate journalists who are saying uncomfortable things, to identify whistleblowers.

This can have two effects, one being to directly abuse state power in relation any individual, the other being to frighten or chill individuals from taking risks.

11 Do we need to think about personal security as different from state security?

Promoting personal Internet security is highly valued by governments as it reduces risks of criminality, viruses and exploits.

However, mass surveillance techniques – particularly Operation Edgehill – run counter to personal security. Parliamentary and ministerial oversight failed to identify this risk, or deemed it acceptable, arguably because no public debate took place.

Very simply, the current situation prioritises state security over everyone's personal security.

12 How do we regain the trust of the public and ensure that our security services are accountable to our democratic bodies?

Courts have been very consistent that, while there is a scale of intrusion, machine recording and examination are forms of surveillance.