How surveillance and privacy should be balanced.

Dr. Julian Huppert

09 June 2014

Summary: the practical steps that can be taken to ensure that there is a balance between surveillance and privacy: from a review of current powers, the release of annual Government transparency reports, effective oversight, the use of judicial - rather than political - authorisation, the re-classification of surveillance data based on how intrusive it is rather than how it is collected, and how necessity and proportionality can be built into the surveillance authorisation process.

- Long-term policy and legislation struggling to keep pace with technological advances.

- Public now has wearable computing (Google Glass, etc) and Internet of Things will soon come into its own.

- Need to establish core principles which balance privacy and surveillance within statute and policy now, before technological advances and the misinterpretation of old laws makes privacy obsolete.

Privacy & Security

- Before we can fix something, we need to understand how it is broken. I will set out just some of the ways the balance between privacy and security is broken from a legislative viewpoint.

- Legislation is old: RIPA is 2000, Intelligence Services Act is 1994, Telecommunications Act is not only from 1984, but *is Orwellian* 1984.
• Most people with knowledge of legislation accept it is out of date; Joint Committee said it was *woefully* out of date.

• Best example is RIPA and definition of Communications Data. Uses old system of what is written on outside of a letter to access all data about us. This is the perfect example of outdated definitions being misapplied to current technology.

• Biggest challenge in Parliament is raising fundamental principles and human rights in face of fear and fear-mongering. This affects how policy and legislation is developed.

• Public fear does not match reality. Mr Anderson, the Independent Reviewer of Terrorism Legislation:

   “It is often said that the threat from terrorism is over-estimated, and the resources devoted to countering it excessive.

   During the 21st century, terrorism has been an insignificant cause of mortality in the UK. The annualised average of five deaths caused by terrorism in England and Wales over this period compares with total accidental deaths in 2010 of 17,201, including 123 cyclists killed in traffic accidents, 102 personnel killed in Afghanistan, 29 people drowned in the bathtub and five killed by stings from hornets, wasps and bees.”

   Mr Anderson noted the threat is sometimes “exaggerated for political or commercial purposes. It is certainly a powerful rallying-cry for the flourishing security and surveillance industries.”

• **Figures**: 17 billion letters delivered by Royal Mail each year. Sounds like a lot, but roughly 2.4 trillion emails sent every year in UK. More emails sent in just 3 days, than letters delivered whole year.

• Doesn’t include 1 billion tweets, 23 billion Google searches, 70 billion Facebook views, 145 billion text messages, and 160 billion instant messages sent in UK each year. Our online data and communications dwarf our real-world communications; and this trend is set to continue.
• Slightly absurd to compare old-fashioned letters with usual modes of online communication in internet age. But this is principle distinction in our laws. Laws passed during 20th Century.

• Distinction between “content” of communications, and data “about” communications. For postal communications, such data means anything written on outside of the item. You can’t get any more information about post without a warrant. But for online communications it includes:

  o who sent it, where they were when they sent it, what device they sent it with, what they were looking at online before they sent it,

  o who they sent it to, where that person was when they opened it, what device they opened it with, and what that person looked at next.

  o Or, as the Regulation of Investigatory Powers Act [RIPA] puts it: “any data identifying the data or other data as data comprised in or attached to a particular communication”. Incredibly vague definition.

• RIPA passed in 2000, before broadband, before smart phones, before Facebook and before Google had fully taken off. Nobody appreciated metadata could be mined to show

  o our contacts, our habits, our work history, our preferences,

  o our movements, our close relationships, our political and religious beliefs,

  o how we like to spend our time and our money.

• But metadata reveals all this about us, and more besides. Complex algorithms and search patterns reveal facets of our identity and behaviour we may not even be aware of ourselves. This information is a virtual diary of our activity and our thoughts.

• Our police and intelligence agencies can obtain all of this information without a warrant. Without judicial oversight. Without any suspicion of guilt. And with hardly any public debate. Should the authorities be
able to read everyone’s digital diary, without suspicion and without oversight or independent approval?

• Intrusive surveillance within a home or car needs approval by a Surveillance Commissioner. Digital surveillance can be just as intrusive, but due to old definitions in RIPA, there is no need for approval. It is self-authorised.

• Study after study shows human behaviour changes when people know they are being watched. When under observation, we act less free, which means we effectively are less free.

• Creation of permanent records of our daily activities, people realise not only can they be watched now, but can be watched by people in the future subjecting them to retrospective investigation. You might not remember what you were doing on 9th June 2012, but the government does.

• Edward Snowden noted: “The power these records represent can’t be overstated. In fact, researchers have referred to this sort of data gathering as resulting in “databases of ruin,” where harmful and embarrassing details exist about even the most innocent individuals.”

• These are just some of the ways that the system is broken, and the balance between privacy and security is weighted too far in favour of security. What can we do to fix it?

Practical Solutions

• Before we can consider new powers, whether explicitly granted or acquired through new technology, we need a pause. Need proper and full investigation into powers already available to police and security services. Must be done competently and with independence. We should commission independent, post-legislative scrutiny of both RIPA and Intelligence Services Act 1994, and other related legislation, to see how they interact with each other. We would then have a clear, open understanding of where we stand now.
• Only then can we create a policy framework for the future. But, risk that by the time we have done this, technology will have moved on again. This is why such a policy framework must be based on core principles – I have drafted such a policy motion which my party endorsed earlier this year at Conference. Time for a Digital Bill of Rights?

• At its core, this Digital Bill of Rights sets out the practical steps to ensure that Privacy and Surveillance can be properly balanced:

1. The annual release of Government Transparency Reports which publish, as a minimum, the annual number of user data requests made by law enforcement, the intelligence agencies, and other authorities, broken down by requesting authority, success rates, types of data requested and category of crime or event being investigated.

2. The establishment of a commission of experts to review state surveillance and all recent allegations from the Edward Snowden leaks, with specific scope to:
   b. assess the implications for privacy and internet freedoms of Project Tempora and other programmes revealed by the Snowden leaks, and consider alternatives to the bulk collection of data
   c. review powers, scope, appointment and resources of oversight committees, commissioners and tribunals
   d. consider the use of judicial involvement and approval for surveillance and for access to communications data and metadata likely to reveal sensitive personal data, and
   e. publish its findings and recommendations.

3. The Government to define and enshrine the digital rights of the citizen to protect from overreach by the state, through:
   a. Ensuring that powers of surveillance, accessing data, and accessing new technologies are not extended without Parliamentary approval
   b. Ensuring that government does not undertake the bulk collection of data and only accesses the metadata or content of communications
of an individual if there is suspicion of involvement in unlawful activity

c. Ensuring that oversight of government surveillance is independent, informed, transparent and adequate

d. Supporting a prompt, lawful and transparent framework for data requests across jurisdictions and between governments.

• Long term, we should sign up to the international principles on the application of human rights to communications surveillance. The thirteen principles are legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, transparency, public oversight, integrity of communications, safeguards for international co-operation and safeguards against illegitimate access.

• Where data is considered intrusive, it should be accorded the same statutory protections as intrusive surveillance under RIPA. There is an urgent need for a review of the definitions used in RIPA, and for inclusion of new hierarchy of data types based on how intrusive each type of data is; that hierarchy can then be given corresponding protection.

• Even the limited protections we have circumvented by information laundering: process by which national legislation is bypassed by means of the sharing of information or reciprocal surveillance programmes with the security and intelligence services of other nations.

• One of biggest problems we face is internet knows no boundaries, and cares little for jurisdiction. Current distinction between internal and external communications, when many servers are based overseas, makes a mockery of the limited protections in place for our citizens.

• The emphasis of our policy and legislation needs to move away from the method of collection of the information and towards how sensitive that information can be, with corresponding judicial or other controls on accessing such sensitive or intrusive information. At the heart of that new decision-making process, there needs to be an
assessment of necessity and proportionality, so that it is hard-wired into all surveillance decisions. At present the vagueness of the letter of the law is allowed to defeat the spirit of the law.

- Sir David Omand, former head of GCHQ:
  “Democratic legitimacy demands that, where new methods of intelligence gathering and use are to be introduced, they should be on a firm legal basis and rest on parliamentary and public understanding of what is involved”.

- This is heart of the matter. Must ensure laws and guidance for staff of police and security services is clear, and that we ourselves understand framework in which we expect them to operate.

- This is a global issue acknowledged by world leaders.

- Goes beyond civil liberties: economic consequences. Digital economy worth £110bn of GDP. Dynamic market - it can move. People concerned about privacy can move to places like Germany which are protecting it better. Balkanisation of the internet?

- If NSA and GCHQ are breaking the encryption systems that we all rely on – not cracking them afterwards, but creating deliberate flaws and back doors – then others can make use of those back doors, too. Potential catastrophic consequences for digital economy, for online banking, and internet as a whole. Must remember internet is an enabling technology for everyone, not just us in the UK.

- Differences in this debate between UK & USA: US Constitution and Bill of Rights sets out contract between state and citizens with bias towards individual liberty and privacy. Explains why debate is so loud in the US but not here. It is time we had a similar Digital Bill of Rights.

**Conclusion** Most policy work in this area is guided by whistle-blowers, select media and civil society groups. Parliament and formal policy makers have been largely silent. We desperately need more experts in Parliament who can speak up on this issue, we need long-term strategic thinking on this policy area, we need strong institutions with independent oversight, and we need all of this to be underpinned by a Digital Bill of Rights. Only way to ensure that the technology we rely on is not turned against us.