Submission to ISC Inquiry

by Lord Strasburger

1. In January 2014 President Obama said to his country and the world "Our system of government is built on the premise that our liberty cannot depend on the good intentions of those in power. It depends on the law to constrain those in power."

2. In the UK, the Snowden disclosures have confirmed that the legislation intended to constrain intrusive surveillance of its citizens by the State is not fit for purpose. In addition, scrutiny of the security and intelligence agencies which is supposed to protect the privacy and liberty of the British people has comprehensively failed.

The difference between watching anybody and watching everybody

3. No sensible person would deny that in the case of those who are reasonably suspected of planning or committing the most serious crimes the authorities need to be able to intrude, deeply, into their private communications, subject to safeguards.

4. However, this power should not be extended to bulk surveillance of the entire population, turning us all into suspects in the manner of authoritarian regimes that we rightly deprecate. That would be a serious and disproportionate intrusion into the privacy of law-abiding citizens.

5. Yet that seems to be exactly what has happened. The Executive appears to have taken for itself the ability to record and store on an industrial scale the private communications of innocent citizens through GCHQ's Mastering the Internet programme.

No permission from the public

6. This has happened without the knowledge or permission of the public and their representatives in Parliament, both of which are essential prior conditions in a democracy for such a significant invasion of our collective privacy. Indeed it seems that even the Cabinet and the National Security Council were unaware of Projects Tempora and Prism until Snowden revealed them.

7. In the words of a former Cabinet Minister "The State should not feel itself entitled to know, see and memorise everything that a private citizen communicates. The State is our servant."

8. The securocrats in the Home and Foreign Offices appear to be pursuing an agenda that will lead to the total surveillance of all citizens. The fact that technological advances have made this feasible, way beyond the imagination of parliamentarians when they passed RIPA, is no reason why it should be permitted.

Does mass surveillance improve public safety?

9. We are told that projects like Tempora are essential for the protection of 'National Security', but no evidence has been presented to show that mass surveillance makes a significant difference to our safety.

10. In the US, where debate on security issues is commendably more open than in the UK and where a similar assertion was made by the NSA, the 54 cases they initially cited where "mass surveillance has disrupted plots at home and abroad" were found on examination in almost all cases to have been uncovered by more traditional surveillance of particular phones and email addresses.

11. The need to protect 'National Security' is repeatedly cited to justify all manner of measures that assault our civil liberties. It is an illuminating fact that of the 550,000 annual requests for access to communications data made under RIPA by the security and intelligence agencies and the police, the vast majority are not about terrorism and involve no threat whatever to the nation's security. In the words of a former Shadow Home Secretary "The very liberties we seek to preserve must not be sacrificed on the alter of National Security."

12. The Home Secretary and others have sought to justify mass surveillance on the simplistic basis that if you are looking for a needle in haystack, first you need the haystack. To continue with this metaphor, looking for a needle in a haystack is hardly helped by adding more hay, in this case thousands of times more hay.

13. Even with the benefit of cutting edge technology to filter the massive silos of private data that GCHQ is collecting, the inevitable consequence must be an avalanche of 'leads', almost all false, that cannot possibly be followed up and which distract the agencies' finite resources away from the real suspects. Something similar led to the failure to prevent the 7/7 bombings in London despite one or more of the bombers being known to the authorities as a potential threat long in advance of the atrocities.

Current legislation

13. The relevant UK Acts – the Regulation of Investigatory Powers Act (2000), the Intelligence Services Act (1994), and the Human Rights Act (1998) – were all written in the last century.

14. Their authors and the parliamentarians who passed them could not possibly have imagined the exponential growth that has since taken place in the use of telecoms and the Internet and how technology has become such an integral and intimate part of most citizens' lives. All three Acts were passed long before the advent of the iPhone, Facebook, Twitter, 3G and 4G, mobile banking, internet shopping, and many other technologies that are now part of everyday life. The three Acts cannot, therefore, properly regulate the monitoring by the agencies of these and future services.

15. GCHQ has stepped into this legal void and may not be breaking the law because it does not need to. RIPA has built-in loopholes – Section 8 para 4 and others - presumably deliberately inserted. These have been exploited for many years by the security and intelligence agencies, and signed off every six months by acquiescent Secretaries of State, to provide legal cover for massive intrusions into everybody's private affairs, intrusions about which we have only just learnt courtesy of Snowden.

Oversight of the agencies, or lack of it

16. As to the much vaunted oversight bodies that are supposed to protect the public from over-zealous behaviour by the security and intelligence agencies, for years they have all failed to be aware of or raise the alarm about mass surveillance by GCHQ. Several Foreign Secretaries and Home Secretaries, the Intelligence and Surveillance Commissioners, the ISC and the National Security Council have all detected nothing untoward in mass collection and storage of citizens' personal private data without the knowledge and permission of the people and their Parliament.

17. According to some of Snowden's documents, GCHQ considers the legal framework in the UK to be more 'flexible' than that which the NSA faces in the US and it also believes that the UK bodies that scrutinise its activities are 'sympathetic'. A senior GCHQ lawyer is quoted as saying "We have a light oversight regime compared with the US. Our Interception Commissioner has always found in our favour."

Metadata and content

18. The ISC asked for opinions on the difference between communications metadata and content. These days metadata about a communication is so revealing about the subject's lifestyle worries, predilections and opinions that there is little distinction from the content. This implies that a more rigorous approval regime is now required for the more intrusive types of enquiry by the State into a person's communications data.

Future risk

19. Once this enormous treasure trove of copies of the private and personal data of all UK citizens has been created, who can guarantee that a less benevolent future government will not abuse it at great cost to citizens? If information is power, privacy is freedom.

The way forward

20. The government must abandon its patronising and arrogant stance towards the public on matters concerning security. Assertions along the lines of 'Trust us' and 'We have the best oversight in the world' are not sustainable now that those in power have been shown to be untrustworthy and to have failed spectacularly to oversee properly the security and intelligence agencies. The USA has much more open arrangements without any risk to essential secrecy; why cannot we?

21. There must be a major public debate in which the government must fully engage, as is happening in the USA, about how much privacy we are prepared to sacrifice for the alleged gains in safety, what the intelligence agencies may and may not do, how compliance with the new rules will be policed by Parliament and how the existing legislation needs to be modified or replaced. A UK Bill of Rights could well be recommended.

22. The ISC's Inquiry cannot possibly substitute for that public debate, given that the ISC is widely perceived as an apologist or spokesperson for the security and intelligence agencies.

23. A Royal Commission is probably the only approach that will command the respect and confidence of the public.

24. In the meantime, the ISC must be seen to be asking the security and intelligence agencies much more probing and awkward questions, and rejecting unsubstantiated or evasive responses. That will require a different membership of the ISC to include those with the required technical skills and a more sceptical outlook.

About the author:

Paul Strasburger has sat in the House of Lords as a Liberal Democrat peer since 2012. In 2013 he was a member of the Joint Select Committee on the draft Communications Data Bill. Previously he was not a politician, but was an entrepreneur and spent 20 years in the IT industry.