Intelligence and Security Committee – Privacy and Security Inquiry

Written evidence from:

Dr Julian Richards[1], Centre for Security and Intelligence Studies, University of Buckingham

Re: ISC8/026 of 13 January 2014

Executive Summary

1. The state needs to be able to continue to ensure strong intelligence and security in the face of grave threats to national security, providing it can ensure that it is assessing those threats accurately, and that it is exercising its powers in a fully authorised and audited way. In many ways, the advent of the internet should not change this equation: it is just a way in which people who would wish to do us harm communicate and interact with one another in the modern age. Consequently, the state needs to have advanced surveillance capabilities against communications on the internet in the same way that it has tapped telephones and conducted other forms of surveillance in the past. We need to look at this issue through the other end of the telescope: we need to think about what intelligence the state needs to be able to meet its national security requirements, while still fulfilling the rights to privacy and liberty; rather than the specifics of the technologies that underpin that intelligence-gathering. We need to think "ends" rather than "means".

2. The nature of modern transnational security threats is very "network-oriented", and targets are embedded in civil society rather than in military or diplomatic milieux. Like it or not, security agencies need to have advanced capabilities in "target development" and "target discovery" if they are to develop leads, spot emerging threats and protect us at the levels we demand.

3. At the same time, it is accepted that the nature of the internet means that the state potentially has greater powers of data-gathering and mining than it has ever enjoyed before, and this means that privacy considerations do become more complicated. There is a strong need for a properly informed national debate which redefines our understanding of core concepts, many of which are being misrepresented currently by sections of the media and other commentators. In particular, the difference between "mass surveillance" and mass "data collection" – which is often obfuscated currently – needs to be clearly defined and understood. Similarly, the requirements of national security in contemporary Britain and the levels of surveillance and target discovery that properly meet those requirements, should also be revisited such that the public can have trust that necessity and proportionality are being applied appropriately.

4. On the legal front, I believe that it is not necessarily a truism that the massive advance in information and communications technology inevitably means that legal instruments such as RIPA are now defunct. We have many old laws in this country that are still very applicable. The changes that RIPA made to IOCA and similar previous laws provided a degree of future-proofing in my

[1] Dr Richards has been Co-Director of the Centre for Security and Intelligence Studies at the University of Buckingham since the centre's formation in 2008. Prior to that, he worked for nearly 20 years in a variety of roles at GCHQ in Cheltenham.

opinion. With that said, I believe it is time to conduct a review of whether the surveillance laws, and the oversight process delivered by the ISC, are still fit for purpose. It is right and proper that a modern liberal democracy does that from time to time and that the public can continue to have confidence in the system.

Details

- *What balance should be struck between the individual right to privacy and the collective right to security? How does this differ for internet communications when compared to other forms of surveillance, such as closed-circuit television cameras? To what extent might it be necessary and proportionate to monitor or collect innocent communications in order to find those which might threaten our security? How does the intrusion differ between data (the fact a call took place between two numbers) as opposed to content (what was said in the call)?*

5. I subscribe to the Hobbesian view that we have a social contract with the state, whereby we surrender some of our individual and collective rights to privacy in exchange for a properly balanced and directed service of security. However, as the Human Rights Act (HRA) properly stipulates, these rights should only be transgressed where there is sufficient necessity (which should be restricted to actions by the state confronting the highest security threats only, in my opinion) and should only be done so in a way that is proportionate to those threats.

6. Taking these in turn, the necessity part of the equation depends on having an accurate and measured understanding of the nature and extent of security threats facing our society. I believe that the National Security Council process instituted in 2010, within which the National Security Risk Assessment is an integral part, is a sound process and should provide a proper understanding of the level and extent of security threats confronting the UK, providing it is updated regularly and efficiently.

7. The second part of the necessity equation relates to changes in society. Specifically, this is about a combination of changes to information technology; and changes to the nature of national security threats. The issue of the technological environment is an extremely important issue here. We know that communications behaviours and technologies have changed enormously in recent years, and continue to do so at a bewildering pace. That means that, in order for the state to deliver security to its citizens through intelligence-gathering, it needs to put in place surveillance capabilities which successfully tackle the technological challenges. This may mean that increasingly expensive and sophisticated surveillance architectures *are* needed, if we are not to be left dangerously exposed to the threats we face. It makes no sense, in my view, for the state to expect everything to remain the same and to be able to continue to be able to gather good intelligence against security threats without updating, upgrading and developing its capabilities in response to target behaviour. Sometimes it might need different approaches also, as were proposed in the draft Data Communications Bill (see below).

8. As we know, national security threats have changed in nature and scope since the end of the Cold War and under globalisation. Most high-priority security threats (such as terrorism, organised crime and weapons proliferation) are now embedded in civil society rather than in diplomatic or military milieux. The targets are hiding amongst commercial organisations and members of the public, and consciously so. I believe this means there is a necessity for the state to have to cross the line – sometimes and in a properly controlled way - into the realm of private communications, in order to chase down those targets that wish to do us harm.

9. The nature of the contemporary threat means that the intelligence and security agencies have to undertake a lot of "target development" work. The much repeated accusation that the security agencies are going on fishing exercises rather than targeting only those that we know to be threats, reflects, in my view, a fundamental lack of understanding of modern technologies and of the target development process. Iain Lobban has aptly tried to convey analogies of needles in haystacks. The state cannot go after the right targets if it has no way of uncovering which are those targets from within the mass of civil communications. This does mean that there will be some collateral intrusion into innocent people's data, but with the right tests of necessity and proportionality applied, and the right oversight regime, I see no reason for the public to be unduly concerned. With the right control regimes in place, including vetting of personnel and the gathering of database-query audit data, there should be a greatly minimised risk of rogue fishing exercises.

10. On this question, I think it is right that data communications are seen differently from content. Those familiar with intelligence know that analysis of data communications can be enormously important to target development, and often to actual finished intelligence. SOCA (now the NCA) said that most of its major organised crime investigations have been underpinned by access to this data. It allows the security agencies to make informed decisions about which people's communications are appropriately subjected to further intrusive analysis, and which are not. Modern security threats are essentially networks, and communications data constitutes the most important raw material for network analysis. I subscribe to the view that, while the gathering and analysis of data communications clearly does entail a degree of intrusion into privacy, it is vastly different and less intrusive than gathering and analysing content. The latter is where the difficult questions need to be asked, and rightly so. The current system in these areas works as well as it can, in my view, and provides protection against disproportionate intrusions into innocent peoples' privacy. I see no reason to change the principle of this approach, although I do accept that the line between metadata and content needs to be continually reviewed in the face of changing communications technologies.

11. This brings us on to the question of proportionality. As mentioned above and in the evidence I gave to the parliamentary committee on the draft Data Communications Bill, I personally believe that intrusive capabilities of this nature should be restricted to use against the most serious of crimes and to national security issues such as terrorism; not to local authority requirements such as tax collection. The latter, in my view, is a disproportionate use of this intrusive technology. A dangerous weapon of this nature should only be used sparingly. Secondly, we must have solid and respected systems of authorisation and oversight in place which ensure that the state is gathering and analysing personal data only on the highest national security priorities, and is doing so in ways which are entirely proportionate to the threat in question. Intrusion into innocent people's data should be minimised as far as possible, but I am firmly of the view that there is a frequent and

sometimes perhaps deliberate confusion in parts of the public media at the moment between “collection” of data and “surveillance”. I do not at all subscribe to the view that the gathering and databasing of large amounts of communications data for target development purposes (querying of which is scrupulously controlled and audited) is in any way equivalent to “mass surveillance”, as some commentators are apt to suggest. It is a dangerous misconception and should rightly be the subject of an informed and developed public debate.

12. Finally, I am firmly of the opinion that the rise of social media and enhanced data footprints generally have meant that the public has a complex and sometimes very paradoxical relationship with its personal data. Many of us freely post quite sensitive personal information on to social networking sites, and many are not unduly perturbed when commercial organisations use very sophisticated data gathering and mining techniques to model quite sensitive assessments and predictions about our personal desires and predilections. (These processes use not only data communications, but content also in some cases.) Yet many of those same people are deeply suspicious of the state using the same sorts of techniques to model security threat behaviour and impacts, with a view to protecting us from harm. We need some more research and a properly informed national debate on our rights to and expectations of privacy in the information age, and where the boundaries around those rights should be situated. This should encompass not only the actions of the state, but also of commercial organisations with whom the public is interacting. The landscape has changed radically, and I believe that none of us really has the right answer yet as to where the balance between security and privacy should be drawn. I believe that statement *does* also apply to the security and intelligence agencies, who have been establishing their capabilities within something of an intellectual vacuum on these issues. In a sense, they could do nothing else as they have had to get on with the business of reacting to technological changes and continuing to gather intelligence while the technology marches on. Keeping within the law (as I am sure the security agencies have been doing) is not necessarily always the same as being morally and ethically right.

13. On the question of whether internet surveillance should be treated differently from other forms of surveillance, I am not convinced that it should be, provided the same tests of necessity and proportionality apply. There is a question of the difference between public and private spaces and the expectations of privacy across both, but these questions are currently applied under RIPA to traditional forms of surveillance, and I see no reason not to apply the same principles to surveillance on the internet. There is a difference between private communications and essentially public “spaces” on the internet (such as open social networking sites), and I see no reason why the same rules of necessity and proportionality cannot apply there, as apply to surveillance in the physical world. In a sense, we might be looking at this through the wrong end of the telescope. The question is how we gather good and productive intelligence, in a proportionate way, against security threats; not the various technologies and modes of communication that the threats may use. We need to think “ends” (in the shape of good intelligence leading to good security) rather than “means”. The same principles should also apply to use of other surveillance technologies, such as CCTV cameras, for example.

- *Whether the legal framework which governs the security and intelligence agencies’ access to the content of private communications is ‘fit for purpose’, given the developments in information technology since they were enacted.*

14. There are two aspects to this. Firstly, I believe the RIPA and HRA framework is still largely fit for purpose on authorisation of surveillance measures, even through the recent technological changes. In the latter part of the 1980s and early 1990s, the Interception of Communications Act (IOCA) quickly became problematic as it was based on communications nodes rather than the targets using them, and mobile technology was starting to make a nonsense of this methodology. RIPA shifted the focus to the subject of the surveillance and was thus applicable across a range of surveillance techniques. I personally believe that this gave RIPA sufficient future-proofing and allowed it to be applicable, even as we moved from the mobile revolution into the more widespread information revolution. Many are currently saying of RIPA what was said of IOCA: that it has become outdated and inappropriate in the face of technological changes. I don't actually accept this argument and feel it could be a false comparison (although I do think it is right and proper that it should be reviewed, if only to improve public confidence in surveillance law). Part of this relates to whether one feels the internet is "different" from other forms of communication. As discussed above, at one level I don't see why it should be: it is merely a new method through which people communicate. We need to gather intelligence on high priority targets, and we need, in my view, to be able to do that across any forms of communication that they may use.

15. The second part of the question, however, relates to the state's ability to gather sufficient amounts and the right form of communications data from the massively burgeoning public network, in order to be able to continue to do target development work to an effective degree. Here, I do agree with the Home Office's argument that new legislation is needed (in the shape of a Data Communications Bill) to allow the state to be able to continue to gain access to the relevant data with the cooperation of the network service providers themselves. Without new legislation of this sort, the state is already at high risk of being left further and further behind in its ability to track and develop intelligence against contemporary transnational threats such as terrorism. This makes no sense at all, and seriously erodes the social contract between state and citizen. Clearly there are risks here of the state appearing to expand its intrusiveness into private communications. Again, however, I believe that a combination of restricting the use of these capabilities to the highest national security priorities; and ensuring that proper authorisation and oversight is used throughout the process, should rightly allay any concerns.

- *Proposals for specific changes to specific parts of legislation governing the collection, monitoring and interception of private communications.*

16. My proposals on the legislative front would be as follows:

- Continue attempts to develop a new Data Communications Bill, allowing state security agencies to be able to access communications data at volume from the service providers.
- Conduct a formal review of RIPA with a view to updating it where appropriate, but focusing on those areas where it is definitely (rather than theoretically) unfit for purpose in the face of technological changes.
- Conduct a formal review of the ISC and associated oversight regime.

17. In addition to actual legislative measures, I do favour a discussion about whether the ISC provides sufficiently accepted and trusted mechanisms for overseeing the security and intelligence

agencies. I think a debate on this issue would help to raise confidence that the state was taking the question of oversight very seriously. In the meantime, I think the ISC should be seen to be conducting a deep and wide inquiry into the very questions we are dealing with here, including extensive debate with the intelligence and security agencies themselves so that they are not left operating in a vacuum. This is the sort of thing that a modern, liberal democracy should be doing. I believe this debate is underway and I fully support it.

Julian Richards
1 February 2014