Evidence for the Intelligence and Security Committee of Parliament[1]

Submitted by Professor Sir David Omand GCB
Visiting Professor, Department of War Studies King's College London

(a) **What balance should be struck between the individual right to privacy and the collective right to security?**

1. The invocation of a balance in relation to collective 'rights', although useful shorthand, is problematic since it implies the more of one for society must logically imply the less of the other. That is not necessarily the case with security, a condition that provides the fundamental basis upon which other rights can be more easily secured. A State that is suffering insecurity will be badly placed to deliver the protection of other rights, including privacy. I define **Security** as *a state of confidence* that the major risks facing the public at home and when abroad are being managed satisfactorily - so that people can make the best of their lives, and live freely (that is, with their essential democratic freedoms and rights protected) and with confidence (the public uses crowded spaces, business has confidence to invest, international travel and trade is possible, and markets are stable). Around the world we can see all too readily countries where this condition fails and where basic human rights suffer as a consequence.

2. What is important is that our public has that confidence in the way that the UK government goes about taking action to manage the major risks that affect us, including in this context the extent to which the State has to intrude upon both the privacy of any individual and that of fellow citizens. That overall level of confidence will have several components.

a. One component is confidence that there is a sound and up to date legal framework within which the executive and judicial authorities must act (and the confidence that such law can be readily accessed and understood if needed – there can be no secret law[2]).

b. A second component is sufficient confidence that those taking risk management decisions (Ministers, senior officials and police officers) share the values of a free and democratic society and that they apply ethical

[1] In response to the Clerk's call for evidence dated 11 December 2014
[2] As appears to have been the case with 'warrantless interception' in the US authorized by the US President under the Patriot Act

principles in their work. A suggested set of such principles for interception is annexed to this note[3].

c. A third component is confidence in the adequacy of the checks and balances on the exercise of the State's coercive powers to reduce the likelihood of abuse of power and illegal behavior through the work of the Committee and the Commissioners and through the internal processes of warranting and control within the intelligence agencies and their parent Departments.

d. A fourth component is confidence that the major threat assessments that justify both the maintenance of intelligence capabilities – and the relevant *jus ad intelligentiam* – and their application to specific cases – and *jus in intelligentio* – have been objectively and fairly evaluated.

3. I draw the Committee's attention therefore to the most recent UK opinion poll[4] that bears on the subject that shows clearly that the British public has such confidence in the system. Although there is certainly a minority that is concerned over intrusions into privacy, the poll shows a large majority of adults in the UK (71%) think that the government should "prioritise reducing the threat posed by terrorists and serious criminals even if this erodes peoples' right to privacy". The same poll shows around 2/3 of adults think that British intelligence agencies should be allowed to access and store the internet communications of criminals or terrorists and around 2/3 also back them in carrying out this activity by monitoring the communications of the public at large. Indeed, most people expected such surveillance to be in place.

4. I conclude that the public as a whole approves of the 'balance' currently being struck.

How does this differ for internet communications when compared to other forms of surveillance, such as closed circuit television cameras?

5. There are at present very different laws regulating these two forms of surveillance, for historical reasons. As technology advances, for example by enabling sophisticated facial and pattern recognition software to be applied to the visual images captured digitally by advanced high-definition CCTV, then its use will become more often a case of directed surveillance as already defined

[3] See David Omand, *Securing the State,* London, Hurst, 2010, chapter 10.
[4]TNS-BMRB, Polling 23-27 January 2014, www.tns-bmrb.co.uk/news-and-events/britons -give-safeguarding-security-a-higher-priority-than-protecting-privacy, accessed 4 Feb 2014.

under Part II of RIPA2000 and as already applies to some CCTV use. It may be that in due course there should a review of the working of Part II in the light of such developments, and the associated Codes of Practice, for example to examine the level at which such directed surveillance may be authorized. But the distinction in RIPA2000 between Part I – interception, broadly speaking – and Part II – directed surveillance - remains in my view a valid one from the point of view of the legal construction of that legislation and the complex interaction with other relevant legislation.

To what extent might it be necessary and proportionate to monitor and collect innocent communications in order to find those which might threaten our security?

6. 'Monitoring' must be distinguished from 'collection' (or 'access', in many ways a more appropriate term). A category error has crept into much of the recent public debate over the material stolen by Edward Snowden and passed to journalists of not distinguishing bulk access to the internet – which the UK certainly does have for example through transatlantic cables[5]– and so-called 'mass surveillance' which it does not conduct. I hope that the Committee will be able to produce an authoritative account of this distinction.

7. It is important that the public be reassured that we are not being monitored as a population and being subject to mass surveillance, and be reminded that it would be unlawful for the intelligence agencies to conduct this. Mass surveillance is about pervasive observation or monitoring of the entire population or a substantial sector of it. Observation implies observers, human beings who are examining the thoughts and actions of the population.

8. GCHQ, in pursuit of its foreign intelligence mission (the Committee will be very aware of the need to assess risks posed by returning British jihadists who have been fighting in Syria) must in my view continue to have bulk access to large volumes of traffic on the internet. The necessity for this stems from the nature of the modern packet switched networks, the exponential growth of internet traffic and its global distribution.

9. The bulk access will be needed to find the wanted traffic of the small number of legitimate targets – what has been described as the needles in a vast set of internet haystacks. Internal control procedures inside GCHQ must continue to ensure that only authorized traffic and data is examined. More could be done by the ISC to describe how in general terms the system works. The use of the term 'mass surveillance' by commentators with its echoes of the Stasi observing and

[5] As revealed in 1968 by Chapman Pincher in the Daily Express

controlling by fear the East German population is simply journalistic sleight of hand to damn the US National Security Agency and GCHQ by association.

10. The volumes of internet traffic, and the way that communications are compressed, bundled and routed (and increasingly encrypted) will inevitably make real-time access impossible from many large and important bearers. The issue might be addressed by buffering and temporarily storing the digital streams which could then be subject to computer examination and application of selectors[6] to pull out for human analysis the wanted communications data and, where warranted, the content of the communications. For how long such material needs to be stored will need to be kept under review as the technologies change. It should be the minimum necessary to achieve the approved purposes and no more. In my view, it would be a mistaken policy to follow the US example and to seek to retain large quantities of data for very long periods before selection and analysis.

How does the intrusion differ between data (the fact that a call took place between two numbers) as opposed to content (what was said in the call)?

11. It has always been possible to derive intelligence from the fact of a telephone call having taken place. The calling number, called number, length of call and their location (originally through the location of the telephone exchange; today through the location of cell towers) has provided generations of police officers for example the ability to locate missing persons, test alibies and pursue investigations without the need to intrude upon the content of conversations. Where the data indicates that content may be necessary to the investigation and its access would be a proportionate response in relation to the seriousness of the matter being investigated then a case for a warrant can be considered. But that is only in a minority of the cases. So the existence of the distinction, enshrined in RIPA2000, is itself a major protection from privacy intrusion.

12. The same arguments, *pari passu*, applies to the work of the intelligence and security agencies in pursuit of their legal purposes[7]. The Guardian for example has not explained to its readers the important difference between **the strict UK legal definition of 'communications data' and the much looser concept of 'meta-data' used especially in the United States to refer to data use by**

[6] Such as the Internet Protocol (IP) address of a suspect's mobile device

[7] E.g. Intelligence Services Act 1994: In the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; in the interests of the economic well-being of the United Kingdom; and in support of the prevention or detection of serious crime.

powerful modern tools when data mining from internet and social media activity.

13. It is the case that with many internet forms of communication (such as social media) it is possible technically to derive much more intelligence about a suspect than could be gleaned from studying the traditional communications of previous eras. Such 'meta-data' as it is called is widely culled by the private sector and sold on for the purposes of marketing of products and services. The internet user implicitly consents to this intrusion as part of the small print conditions for using the service concerned and has in some cases the option of privacy settings to prevent such use of their personal information. Naturally, I would expect the intelligence and security agencies to adopt such techniques to help achieve their approved purposes – but to apply them to cases only once they have the necessary legal authority under RIPA2000.

14. Channel 4 News, for example, got themselves tangled up[8] over the Dishfire database that NSA has, of information culled they say from millions of text messages a day. Were NSA to allow GCHQ analysts to use a database containing such data, as the Committee will be well aware, those analysts could only access it in a way compliant with the narrow UK definition in RIPA2000; if they want to access any content held by the US on a database such as Dishfire they would have to have the relevant Secretary of State warrant.

15. My understanding is that a GCHQ analyst is authorized to treat as communications data only material specifically meeting the legal tests set out in RIPA2000 e.g. the IP address of the suspect machine or email address of the user, when and from where the communication originated, and the server identity being accessed[9]. Thus the analyst can find out under the rules for communications data that the suspect accessed Google - but not the questions asked; that the suspect accessed Amazon but not what was purchased.

16. In shorthand, this is referred to as internet communications data up to the first slash as in www.google.com/ .... Everything beyond that is content for which the analyst requires a warrant from a Secretary of State. A similar position arises with emails - the email address to which an email is sent is considered communications data but not what is in the title of the message and nor the message itself.

(b) **Whether the legal framework which governs the security and intelligence agencies' access to the content of private communications is 'fit**

[8] Channel 4 News, 17 January 2014.
[9] RIPA Section 2(9)d

for purpose', given the developments in information technology since they were enacted.

17. I was PUS in the Home Office when the RIPA Bill was developed and I can assure the Committee that great care was taken by Parliamentary Draftsmen to make the definitions of Part 1 covering interception technology neutral. The argument that because RIPA 2000 predated Facebook and social media and so-called 'scraping' technologies the Act must inevitably be inadequate is bogus. Any case for change in the provisions must be argued on merit.

18. Indeed, those who argue for change should be careful over what they wish for. I referred earlier in this note to the important difference between the strict UK legal definition of 'communications data' and the much looser concept of 'meta-data'. It would in my view be a mistake – since it would weaken protection against unnecessary intrusion – to change the RIPA2000 definitions by modernizing them to align with modern meta-data techniques.

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

19. The care that was taken to make the legal definitions in RIPA2000 technology neutral is in part responsible for the complication of the wording of the Act. That places greater importance on the Codes of Conduct written in accessible plain English for the exercise of the powers under RIPA2000, codes which are publicly available on the .gov website. These Codes are presented to Parliament and are an essential – but alas much neglected – source of reassurance about how RIPA2000 operates in the internet age, and for example how legally privileged material and journalistic material must be handled if inadvertently intercepted and the key role of the Interception Commission.

20. I suggest that the Committee leave the Act itself and focus on the Codes and where they could be usefully expanded and updated to give Parliamentarians, the media and the interested public a much clearer view of the purposes for which interception is authorized (with examples), how modern interception has to work in a packet switched internet age, the part GCHQ as a foreign intelligence agency plays in supporting some domestic investigations, and the treatment of meta-data in relation to the RIPA2000 communications data definitions. In my view, more could have been done over the last few years of rapid technological change to explain these matters to the public, and the Codes of Practice could provide an authoritative vehicle for filling this gap.

21. A further media confusion that could be cleared up in this way is over the American legal distinction between US and non-US persons. The US Constitution

protects the privacy of US persons anywhere in the world – the main issue that motivated Snowden - but does not offer the same protection to non US citizens. UK law on the other hand does not discriminate between British citizens and others over authorizing intrusive investigative powers. As the Committee knows RIPA2000 makes the geographical distinction between the communication of persons in the British Isles - where the Home Secretary is the Secretary of State accountable to Parliament - and persons overseas or communicating overseas - where it is the Foreign Secretary who is accountable. The UK position is in my view actually more compatible with the European human rights tradition as incorporated in the UK Human Rights Act in terms of privacy rights being universal.

Professor Sir David Omand
King's College London
7 February 2014

Annex

There must be sufficient cause to justify the acquisition of intelligence capabilities. Any tendency for the secret world to encroach into areas unjustified by the scale of potential harm to national interests has to be checked. British legislation already does this satisfactorily in terms of the limited purposes for which intelligence can be collected.

There must be integrity of motive. No hidden agendas: the integrity of the whole system throughout the intelligence process must be assured, from collection to analysis and presentation.

The methods used must be proportionate. Their likely impact must be proportionate to the harm that is sought to prevent, for example by using only the minimum intrusion necessary into the private affairs of others.

There must be right and lawful authority. There must be the right level of sign-off on sensitive operations, with accountability up a recognised chain of command to permit effective oversight, both Parliamentary and independent judicial assessment of compliance with the law.

There must be a reasonable prospect of success. All intelligence operations need careful risk management, and before approval is given there has to be consideration of the likelihood of unintended consequences and the impact if the operation were to be exposed or otherwise go wrong and harm innocent parties.

Recourse to secret intelligence must be a last resort. The necessity for using intrusive methods must be demonstrable. There should be no reasonable alternative way of acquiring the information by non-secret methods.