Submission from Rt Hon David Blunkett MP (in a personal capacity) to the ISC Privacy and Security Inquiry Call for Evidence
7th February 2014

Executive Summary

This Executive Summary is to be read in conjunction with the substantive submission.

In giving evidence to the ISC I argue that a balanced and rational debate is required to look at the reassessment of both protection, reassurance, and regular review which is essential to secure continuing legitimacy and therefore consent, a vital part of any free society.

I have already expressed concern about how British citizens can be protected by acceptable oversight and review when other agencies hold data outside the UK, which is then supplied to internal security and intelligence operations, without the normal protections. I am aware that RIPA (section 15 and 16) is intended to give protection in relation to interception outside the British Isles but re-examination in respect of information sharing is necessary. It will be important to ensure that oversight is extended to protect the rights of UK citizens whatever the source of intercepted data.

Section 8.1 of RIPA gives authority for interception of communications of specific individuals providing that a warrant has been obtained, signed by the relevant Secretary of State. The volume of such applications has understandably grown. The ISC will I am sure, wish to examine with Ministers whether the present process remains viable.

Erosion (people going further than was intended) can undermine confidence, and illustrates how important it is to return to these issues regularly. I believe it is necessary to examine for instance 8.4 and 8.5 of RIPA which gives broader authority to collect communications data without reference to specific individuals or premises.

Furthermore, distinguishing between the 'bulk' temporary retention and the debate around updating legislation and powers relating to personal Communications Data is important and should be addressed by this inquiry.

This is not solely a matter of practicality but one of psychology. Unless we reassure the population that every reasonable step is being taken to ensure that those who are employed to secure our well being are doing so within the limits laid down by legislation and are genuinely held to account for their actions, confidence will be eroded.

I believe therefore that the ISC with its new powers should not only demonstrate capability in dealing with the day to day challenges but also make recommendations which anticipate changes of tomorrow, consequent on a five yearly review.

Following President Obama's US initiative I would suggest the ISC take on the challenge of laying out a roadmap for improved transparency and therefore increased confidence. Surely one of the updated roles the ISC can play is to feed into the revisited National Security Strategy, preparation for which the Prime Minister has recently indicated has just begun. For instance, would it be sensible to have a group of 'experts' who worked alongside the Security and Intelligence Services and were in effect arbiters?

Failure to achieve these step changes can only play into the hands of those who would rejoice if on behalf of their citizens, democratic nation states were to lessen their vigilance. Whether public or private, nation state or terrorist grouping, proportional but tough measures must be in place, commensurate with the threat we face.

---

1. The balance between the duty of the State to protect its citizens (both from external and internal threat) and the rights and privacy of individual citizens, has been a central feature of maintaining a free democracy and liberty from oppression since the development of the modern franchise (and in terms of our legal rights, long before).

2. From Jean Jacques Rousseau to John Stuart Mill, what used to be described as the 'dialectic' has stood us in good stead, in maintaining that balance. What has changed in very recent times is not the underlying challenge but the nature of the means both of intrusion into privacy (by government and private enterprise) and the nature of the threat posed.

3. These two elements come together in relation to cyber security. The very means of intrusion becomes in some instances the nature of the threat itself. In this case to Resilience and the potential to dislocate the functioning of modern society. Whether in government or business, it is only now (across the world) that the extent of this potential threat is fully being realised.

4. Equally, the means of dealing with such a threat (alongside more traditional physical attack by terrorists, rogue states or organised criminals), remains in an embryonic state given the extent of current awareness, training and therefore facility to deal with such threat.

5. It is of course the exponential expansion of communication as well as the changed nature of the threat, which gives rise to the fear of interference in the lives of innocent citizens, and the changed techniques by those engaged in security, to match that volume of transmission.

6. From the steaming open of envelopes (the origins of which could be traced) and the ancient switchboards when operators had their ears as well as their fingers on the pulse of what was taking place in their town and village, through to the billions of text and mobile messages (and internet interchange) the world has turned on its head.

7. That is why a balanced and rational debate is required, and a reassessment of both protection and reassurance and regular review is essential to secure that continuing legitimacy and therefore consent, which is a vital part of any free society.

8. Many activists concerned about intrusion and breach of privacy, talk about the relative lack of debate in this country compared with the United States. I think they probably mean 'volume' because in my experience the debate is vigorous, the concerns are taken seriously but as part of our own history and culture, we are not

likely to raise the temperature in the same way as campaigners across the Atlantic, are accustomed to.

9. However, the level of concern demonstrated by recent polling (attached in this contribution) is much less than in the US, even if there is a health warning in respect of the questions asked and the knowledge possessed by the respondents (TNS, Public Opinion Monitor Surveillance Special, January 2014).

http://www.tns-bmrb.co.uk/news-and-events/britons-give-safeguarding-security-a-higher-priority-than-protecting-privacy

10. It does not help however if government Ministers with all the best intentions, keep reiterating that it is 'impossible to give any detail or reflect on the intricacies of these matters because by doing so the very security we seek to facilitate would be compromised' – or words to that effect!

11. For whatever we think about the so called 'revelations' of Edward Snowden (and I think that he is both a thief and a traitor to his country), what has been brought to light changes materially the terms of this debate.

12. What in my view has been revealed is the failure of previous monitoring and review mechanisms to pick up the speed of change as well as the detail of the extended activities of those intelligence and security operations which have over recent years, collaborated through the development of trust into highly effective operations that are prepared to share data and therefore information. It is not to disparage the existing oversight mechanisms to draw the conclusions that greater openness is a prerequisite for mirroring the trust that exists within the system by trust from those whose wellbeing is to be protected.

13. It is not the nature of 'espionage' (so often paraded as being somehow new and therefore revealing) that is the main concern. After all, we have been aware of even friendly countries monitoring communication and seeking to protect their national interests, since the development of the modern state! It is total naivety to believe otherwise!

14. No, this is about the capacity to be able to genuinely protect the innocent from gross intrusion, and at the same time to put in place protective mechanisms for those who because of their position, their history or their significance, require their communication and data associated with them to be secure.

15. In other words, we are dealing with information assurance on the one hand and oversight for where monitoring is necessary, on the other.

16. Oversight by Ministers, parliamentary oversight by the ISC and the role of the Interception and Surveillance Commissioners is undoubtedly robust but within the parameters to which such oversight applies. Equally, there is a complaints procedure through the investigatory powers tribunal but its work is little known and its effectiveness in dealing with complaints substantially in doubt.

17. As indicated above, what was adequate and deemed to be satisfactory in terms of safeguards when we were dealing with traditional telecommunications is no longer satisfactory in the world of what has become known as Meta Data (bulk collection and retention of data but with the intention of, or capacity to, interrogate only a tiny fraction of the total held).

18. Distinguishing between the 'bulk' temporary retention and the debate around updating legislation and powers relating to personal Communications Data is important and should be addressed by this inquiry.

19. It is worth noting that the language used (by campaigners concerned about privacy as well as professionals engaged in Signit and the like) is obscure and often impenetrable. It leaves the bulk of the population outside of the dialogue sought, and therefore either simply frightened by what they are told is being done 'to them' or completely turned off and therefore indifferent. Either way, this is not healthy.

20. Having been responsible for the implementation of the regulation of the Regulatory Investigatory Powers Act (not for the legislation but for the early provisions) I know how difficult these matters are. Best intentions often turn out to create the very concerns which were intended to be allayed. After all, RIPA was there to ensure there was a framework which previously had not existed but by doing so, raised the issue of the porous nature of such boundaries and the controversy about who was doing what to whom. Section 8.1 of RIPA gives authority for interception of content of the communications of specific individuals providing that a warrant has been obtained, signed by the relevant Secretary of State. The volume of such applications has understandably grown (as has the work of the Commissioner reviewing such authorisation). The ISC will I am sure, wish to examine with Ministers whether the present process remains viable.

21. Erosion (people going further than was intended) then later undermined confidence, and illustrated how important it is to return to these issues regularly, to reflect on precisely how safeguards are being implemented, and where tightening up is required. I believe it is necessary to examine for instance 8.4 and 8.5 of RIPA (giving broader authority to collect communications data without reference to specific individuals or premises).

22. I have already (including publicly) expressed concern about how British citizens can be protected by acceptable oversight and review, when other agencies (state or private) hold data, traffic and therefore movement and pattern of communication activity, or material data, which is then supplied to internal security and intelligence operations, without the normal authorisation and therefore the protective process, developed internally. I am aware that RIPA (section 15 and 16) is intended to give protection in relation to interception outside the British Isles but re-examination in respect of information sharing and passive receipt of intercepted information is necessary. It will be important, difficult as this is, to ensure that oversight is extended to protect the rights of UK citizens whatever the source of intercepted data generated by them.

23. This is one of the most difficult aspects of all. It raises the issue as to judgements made about who is formulating the risk analysis and on what basis. What for instance

do our own intelligence and security services lay down as the very basic criteria for concern. This is easy where there is an identified risk, individual or group posing a risk, and therefore an intelligence based approach. When this is not the case, it seems a basic tenet of protecting our privacy that such criteria should be developed and should be available to the intelligence and security committee. Without this, it is clear that 'fishing expeditions' lead to not only unnecessary and in many cases unmanageable trawls but also unacceptable intrusion.

24. The development (and case law arising from) both the Data Protection Act and the Human Rights Act, need to be seen as part of this review, arising as they do since the existing oversight provisions were put in place (general authorisation in the Intelligence Services Act 1994 is clearly in need of revisiting).

25. I have long been concerned that the failure to develop more sophisticated intelligence based approaches mislead all of us (including those deeply committed in the intelligence and security services themselves) to believing they are doing something meaningful when in fact the volume and complexity actually results in them wasting the most enormous amount of time and energy.

26. There is nothing worse than self delusion in relation to believing that a highly complex system is providing important safeguards, when its very complexity is doing nothing of the sort. Let me be clear, when colleagues proclaim that we have the best oversight and review (commissioners) and most thorough system in the world, I concur. The issue is therefore not whether we have taken steps in the past to ensure protection of individual rights and civil liberties but whether they are appropriate for the very changed world that has emerged over the last decade and the challenges of tomorrow?

27. This is not solely a matter of practicality but one of psychology. Unless we reassure the population (and particularly opinion formers) that every reasonable step is being taken to ensure that those who are employed to secure our well being are doing so within the limits laid down by legislation and are genuinely held to account for their actions, confidence will be deeply eroded. In such circumstances the work of those who are protecting us, will be undermined and the legitimacy necessary to ensure backing for their work, will be destroyed.

28. I believe therefore that the ISC with its new powers should not only demonstrate capability in dealing with the day to day challenges but also make recommendations which anticipate changes of tomorrow, and the necessity of putting in place in each (now fixed term parliament) a rigorous and thoroughgoing review of not only how existing safeguards have been implemented but will additionally be necessary in this rapidly changing environment.

29. Greater information to and involvement in the process by Members of Parliament, would assist. An understanding of not only the processes adopted but the challenges of cyber security for the future would help. Government should make resources available to effect this improvement in, at its crudest, education and information for legislators.

30. Of course, on the other side of the coin are those who criticise security and intelligence (and the policing service) for not picking up on basic material available through surveillance. For instance, critics of the analysis of data available in the lead up to the 7th July 2005 attacks on the underground and Tavistock Square. What is lost in such criticism is the understanding of human failure. Time and time again we have been saved by work which has prevented the development of or the carrying out of attacks (physical or cyber). By the very nature of such work, the 'unknown knowns' go unrecognised because an attack that is foiled is an attack that is not known about! There are of course those occasions when it is impossible to prove a negative' so we are in this area dealing with a matter of 'trust'. Again, this is why the psychology of maintaining support for the absolutely vital work of the Services, is so crucial.

31. But there are two other aspects.

32. The first is how well we develop proactive defence mechanisms. It is clear that some nations are devoting the most enormous resources both to predicting and to dealing with threat (particularly that relating to electronic communication). So, the issues under review are not just about 'constraining' or 'monitoring' what our Services are doing but also whether they are being given the resources to develop the protective shield that we require in order that we might not turn on each other at some future date and demand 'why did someone not spot that those threatening us were more advanced, more aware or more technically able than we were'?

33. The second, (and we need to be frank about this) is whether we have the tools to launch pre-emptive attacks.

34. Whether physical or cyber, we are talking about prevention. There is still regrettably a somewhat old fashioned and outdated view that we are talking about 'pursuing' and then 'prosecuting'. Very often we are talking about preventing calamitous events in which prosecution and punishment would be a complete irrelevance (not least because those affected would rejoice rather than be diminished by whatever punishment we could mete out).

35. This is about being realistic in the very changed world and landscape in which our security and intelligence services are operating. It is about the nature of the threat, the intention of those threatening, and the likely outcome of their success.

36. World leaders expect their own Services to protect them from intrusion from elsewhere, as well as expecting respect from those who they count as allies and democratic friends. Businesses understand the issue of 'commercial espionage', and at its most simplistic the theft of Intellectual Property. And those in the real world of business also understand the 'trashing of reputation' which modern communication can bring (often unwarranted), and the way in which competitors set out to destroy business continuity or the success of their rivals.

37. We are therefore dealing with both naivety about the nature of the world that we currently inhabit, and at the same time trying to embed democratic processes to constrain those whose genuine enthusiasm carries them beyond the authorisation we as a democracy have given them, to work on our behalf to protect our life and well being.

38. And then of course there are those who describe themselves as 'ethical hackers'. Self appointed guardians, unaccountable to anyone except themselves. The 'anarchists' of the modern communication landscape. Whilst we rightly concern ourselves with 'the State', it is equally important to understand the power of major multinational businesses (and what they hold about us), and the 'libertarians' who believe that their actions are always justified whilst criticising those of elected governments!

39. Contradictions abound. Questions have been raised as to whether it would be useful to emulate the statement made by the President of the United States, Barack Obama. Clearly this would be the case if there was a road map laid out by the Prime Minister which had concrete proposals which were both practical and achieved the balance between those campaigning on civil liberties and the security services responsible for maintaining those liberties. Although such a proposition is not part of the remit of this review, I would suggest that the ISC should take on the challenge of laying out such a roadmap. Surely one of the updated roles the ISC can play is to feed into the revisited National Security Strategy, preparation for which the Prime Minister has recently indicated has just begun.

40. For instance, instead of those undertaking a review of what has occurred historically, would it be sensible to have a group of 'experts' who worked alongside the Security and Intelligence Services and were in effect arbiters? The presumption here is that such expertise exists and that individuals are themselves free from prejudice or an affinity with a particular point of view. What is certain in my own mind is that 'judges' are not the best people to do this. Their job is an entirely different one. Not least, because our judicial system is based on an adversarial process not on an investigatory or analytical one.

41. Separately, there is the issue of who should hold data, for how long, in what format, as well as patently for what purpose. This has been the subject of much wider debate over several years, including proposed legislative changes (as indicated earlier, in relation to legislation in respect of Communications Data). It is clear from observing the debate inside government that the closer ministers are to the challenges, the more they know and appreciate both the potential dangers and the nature of the counter operation - the more amenable they are to updating authorisation powers.

42. However, the very nature of the changed threat (the nature of technology and how it can be counteracted, as well as methodology in terms of penetration of those wishing to do harm), the more difficult it is to persuade the public. This is indeed a circle which will have to be squared. Winning people over including transnational internet and telecom companies necessitates both greater transparency but also greater honesty about the contradictions.

43. After all, many of those involved in cooperation with the NSA, GCHQ and other agencies, also track (and collate data) on individuals for a whole variety of purposes, including targeted advertising.

44. Breaking down the different types of data retention for a shorter time is appropriate and practicable, and in diffuse rather than centralised form, will help. As will much

clearer rules relating to access, transferability, and of course, regular reviews of justification.

45. Which brings me to the question of the role of the ISC. Failure by oversight bodies on both sides of the Atlantic to pick up the nature of Operation Prism in the United States and Tempora in the UK (we are checking the spelling on this), and wider suspicions that have arisen in relation to other operations, necessitates a rebuilding of that confidence.

46. The extended powers already granted, need to be spelt out more clearly, and if necessary, both additional resources and the power to commission expert investigation, should be granted. Once again, the issue of building oversight mechanisms which command legitimacy and credibility must be paramount.

47. Failure to achieve these step changes can only play into the hands of those who would rejoice if on behalf of their citizens, democratic nation states were to lessen their vigilance, their capability to both prevent and proactively pursue those who would act to damage life, economic and social wellbeing, and the functioning of our democracies. Whether public or private, nation state or terrorist grouping, proportional but tough measures must be in place, commensurate with the threat we face.