Privacy and Security Inquiry

Executive Summary

- Surveillance of the Internet, undercover policing and international intelligence sharing all raise key questions about the effectiveness and propriety of state action.
- Security and rights cannot be 'balanced': the objective in democracy is to maximise both.
- That *everyone*'s communications may be collected without governments needing to show any 'reasonable cause' is the crux of the current controversy.
- Technological changes mean that metadata can be just as intrusive as the content of communications.
- The gulf between official insistence that GCHQ has acted lawfully, while critics argue the opposite, is explained by the broad powers in RIPA s.8 combined with ISA s.3.
- Current law has served the intelligence agencies well but the aim of any reformed legal framework must be to ensure:
    - increased certainty and clarity;
    - the effectiveness and propriety of agency policies and practices; and
    - improved public education.

1. Introduction

1.1 Concern with excessive surveillance did not begin with Edward Snowden: in 2004, for example, the Information Commissioner said that Britain was 'sleepwalking into a surveillance society'. In 2009 The House of Lords Constitution Committee warned that increasing use of surveillance by the government and private companies is a serious threat to freedoms and constitutional rights.[1]

1.2 The Internet is not the only worry: around 50 convictions have now been reversed as a result of police and prosecutors mishandling the undercover policing of environmental protesters, the coroner in the Mark Duggan shooting voiced concern at the role of intelligence in the lead up to his shooting and well substantiated allegations of collusion in rendition and torture by UK intelligence personnel have been heard by the Gibson inquiry. Yet, contrary to the apparent ubiquity of surveillance revealed by Snowden, Lee Rigby's killers were unhindered although known to the Security Service.

[1] Surveillance: citizens and the state.
http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf Jan 23, 2013

1.3 Important questions are raised about the relationship between government and private companies. Given that CSPs are private, how do intelligence agencies access communications? RIPA dealt with this to some extent but we learn now that agencies may also obtain access without the CSPs knowing. Companies have expressed much anger at this which, were it to continue, could modify their willingness to cooperate under RIPA and any future Communications Data legislation.

1.4 International intelligence cooperation is almost entirely secret and not subject to law. First, the only limit on the transfer of information abroad by UK agencies is ministerial discretion (RIPA, s.15). There is no restriction on the receipt of information from abroad (except in the case of torture). Second, cooperation is usually bilateral and any subsequent action is more likely to be disruptive than aimed at arrest and prosecution. Third, although there are formal intelligence-sharing agreements, much cooperation takes place informally between practitioners. Fourth, intelligence sharing is subject to the 'control' principle whereby an agency may not disclose intelligence to a third party without the permission of the originating agency. This may be applied also to external oversight bodies.

2. The ISC would welcome written evidence on the following issues:

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

2.1 This commonly-used metaphor of 'balance' can be misleading. Societies with fewest human rights do not enjoy greatest security; indeed, to the contrary, personal and collective security tends to be highest wherever, such as UK, human rights are well protected. Security and rights are not commensurable, the objective in democracy is to increase both. It is often tempting to argue that 'more' security can be obtained by 'reducing' rights but, in practice, this means that majorities may *feel* more secure if the rights of certain minorities are curtailed. Rather, the concepts of necessity and proportionality should be applied, as in the question below.

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

2.2 In principle, not at all. A crowd can be scanned by face recognition software programmed to seek specific people in the same way that internet traffic is scanned for specific 'selectors' such as names, numbers, places. Both raise the question of what are legitimate expectations of privacy in the modern world. These are clearly shifting, for example, many people

publicise their personal information on social network sites to an extent that would have seemed bizarre only twenty years ago but they *choose* to do it. Similarly, we choose to 'pay' for Google, Microsoft and other services with our personal information. State surveillance, however, is different because, as a result of intelligence, states may arrest and prosecute us in a way that corporations may not. This, arguably, is part of a 'social contract' by which we give up certain rights in order that the state can protect us from security threats.

2.3 However, many states abuse this contract and an essential precondition of democratic status is that surveillance is subject to procedural safeguards and oversight. We can avoid the 1.85m public cctv cameras[2] by never going out and the 8,000 police road cameras[3] by not driving just as we can avoid interception of our communications by never using the mail, telephone or Internet, but 'normal' life would be barely possible. We must retain some right to privacy as we communicate and live publicly. But whereas total surveillance of public space is impossible – it cannot be concentrated into choke points that render collection feasible -- near-total surveillance of electronic communications seems to be in reach; therefore it presents distinctive legal and policy challenges.

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?

2.4 This is the crux of the current controversy: since June 2013 no-one has opposed the idea that *individuals*' communications may be targeted on the basis of some degree of suspicion as warranted by a minister or judge. But the idea that *everyone*'s communications may be collected without there being any necessity for governments to show any 'reasonable cause' has angered many.

2.5 We need to consider how this actually happens: for example, GCHQ collects material from fibre-optic cables as they come ashore from the Atlantic (TEMPORA). Thirty per cent of the 1-2billion records a day collected is immediately rejected while 40,000 'selectors' chosen by GCHQ and 31,000 by NSA based on key words, phone numbers etc. scan the rest. TINT facilitates storage permitting retrospective analysis by the 300 GCHQ and 250 NSA analysts working on 'target discovery' and 'target development'. Content remains on the system for 3-5 days and metadata is stored for 30 days though analysts can store 'interesting' material in another database for up to five years.[4] NSA and US Office of Director of National

[2] https://www.cctvusergroup.com/art.php?art=94 January 23, 2014
[3] 'CCTV cameras on Britain's roads…' *Guardian*, January 24, 2014, 1.
[4] 'GCHQ taps…' *Guardian*, June 21, 2013; 'How NSA can see…' *Guardian*, August 1, 2013, 1-2.

Intelligence (ODNI) said that, using all its authorities, the agency 'touches' 1.6% of internet traffic and that analysts 'look at' 0.00004%.[5] These figures look realistic: if 2 billion records a day are 'collected' and 32 million are 'selected', this far exceeds anything that could possibly be 'analysed'. So, about 80,000 will be 'looked at' which still sounds barely feasible if one accepts that 'analysis', however clever the software, ultimately requires a human being to decide what the communication means.

2.6 President Obama's Review Group wondered whether artificial intelligence software could be developed to enable selective collection in real time rather than requiring storage and subsequent sorting but they admitted they had no idea whether the concept was 'feasible or fantasy'.[6] If governments believe it is necessary to store 'everything' (even if for only 30 days, in order to permit searching *via* selectors) then they need to explain to the public why this is so and establish clear procedures to monitor the process in order to allay public concern. For example, governments have a legitimate need to search data retrospectively in order to investigate the networks of current suspects and for those currently 'unknown'. On the other hand, the attempt to 'collect everything' is arguably so disproportionate to current security and criminal threats that it should be subject to an external audit of legality and effectiveness by a more wide-ranging inquiry than could be conducted within these terms of reference.

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)?

2.7 Police and intelligence agencies have long made use of communications data in order to develop a picture of the networks of those under suspicion and, when communications were by mail or telephone, this distinction was clear-cut. Although the Data Protection Commissioner argued in 2000 that communications data and content should be subject to the same safeguards,[7] agencies do not need a warrant to access communications data (RIPA ss21-25). Metadata is still quicker and cheaper to access than content, but technological advances have strengthened the argument that it is no less intrusive. For example, where someone uses a third party communications provider hosted on her CSP, details of the final recipient can

[5] Joint Statement: NSA and Office of the Director of National Intelligence, August 21, 2013, www.nsa.gov

[6] *Liberty and Security in a Changing World*, December 12, 2013, 173-74 http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf January 20, 2014

[7] Cited in Williams, 2006, *Surveillance and Intelligence Law Handbook*, Oxford UP, 112.

only be found within the content of the data packet.[8] Further, 'relational' software enables the virtual reconstruction of someone's life and movements from communications, travel and financial data which may actually be more revealing than specific conversations. 'Content' may only record 'two idiots talking on the phone.'

b**) 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.**

3.1 It is generally acknowledged that the law has *always* lagged behind developments in communications technology and, to the extent that the latter takes place at increasing speed, this becomes ever more a problem. However, a more specific answer to this question depends on *whose* purpose we are considering. The RIPA framework seems to have served the agencies well, if we are to believe government statements that they have acted legally, and the Communications Data Bill was apparently designed more for the needs of police than intelligence agencies who have greater resources to 'solve' interception issues. But the current law has not contributed to public understanding.

3.2 When the Human Rights Act became effective, RIPA codified the state's information gathering powers and retained the distinction - established in IOCA 1985 - between a warrant for interception of named people and places under s.8(1) and a 'certificated' warrant under 8(4).[9] Six weeks after Snowden's first revelations appeared, the ISC stated that its investigation of allegations that GCHQ acted illegally by obtaining the content of UK citizens communications via the NSA's PRISM programme showed them to be unfounded.[10] Former GCHQ Director David Omand said that 'For Britain, Snowden's public interest justification is thin since subsequent investigation has shown conclusively (that GCHQ) has at all times acted lawfully.'[11] But these reassurances are somewhat weakened by the report that one of GCHQ's 'key selling points' in its financially subsidised relationship with NSA is the UK's more relaxed legal regime.[12]

---

[8] Review Committee on the Intelligence and Security Services, 'On the use of Sigint by DISS,' *Annual Report* 2011-12, 37-110 at p.81. http://www.ctivd.nl/?English January 20, 2014

[9] Cf. Williams, 2006, 74-75. GCHQ reportedly have 10 basic certificates that cover the entire range of their intelligence production. 'Legal loopholes…' *Guardian* June 21, 2013.

[10] ISC, *Statement on GCHQ's Alleged Interception of Communications under the US PRISM programme*, July 17, 2013.

[11] David Omand, 'Edward Snowden's leaks are misguided…' *Guardian*, September 26, 2013.

[12] 'Inside GCHQ…' *Guardian*, August 2, 2013, 1-2.

3.3 But if RIPA does ensure the legality of the agencies' actions, it is not widely understood, for example, former Home Secretary David Blunkett said that RIPA was introduced by Jack Straw 'to provide a framework for what was a free-for-all in a growing but little understood area'.[13] Former Lord Chancellor Lord Falconer said that the Snowden material raised very serious questions about the adequacy of the UK's legal framework for oversight of the intelligence services' work in relation to the interception of communications.[14]

3.4 No enlightenment has come from oversight by the Interception of Communications Commissioner (ICC).[15] The 2004 Report cited an IPT decision of December 2004 upholding the lawfulness of an 8(4) warrant but there was no explanation of the significant differences between the two types of warrant (pp.8-9). The 2010 Report provided a graphic of the warrant authorisation process but this also made no reference to the two types of warrant (p.10). Now it is reported that GCHQ activities are covered by just ten s.8 (4) certificates, we can see this is a very significant omission. Overall, it appears that the reason for official insistence that GCHQ has acted lawfully, while critics argue the opposite, lies in the broad powers in RIPA s.8 when combined with ISA s.3. If the law does not require up-dating, it certainly requires clarification and better explanation as well as improved oversight of those who apply it.

3.5 This can be done without threatening security. For example, the Dutch Review Committee on the Intelligence and Security Services (RCISS) has provided a useful account of why and how selection criteria including key words are used to filter bulk collection. Ministerial permission is granted for a general subject to which the key words are related but not for the precise lists of key words which may be amended daily as necessary. 'Generic identities' are also used and cover a particular 'type' of person or organisation and avoid the need to identify specific individuals. The advantages for the agencies are obvious: the specific names and locations of individuals may not be known, organisations change their names, and people use aliases and multiple channels of communication.[16]

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

---

[13] 'Blunkett calls…'*Guardian* November 5, 2013, 1-2.
[14] 'Security chiefs "exaggerated"…' *Guardian* November 18, 2013, 1-2.
[15] See ICC annual reports, especially re. RIPA Chapter 1, for 2000-2012; 2001 and 2009 could not be downloaded. http://www.iocco-uk.info/ January 20, 2014
[16] Review Committee on the Intelligence and Security Services, 'On the use of Sigint by DISS,' *Annual Report* 2011-12, 37-110 at 88-98. http://www.ctivd.nl/?English January 20, 2014.

4.1 All intelligence legislation - SSA 1989, ISA 1994, Police Act 1997, RIPA 2000 - both empowers and limits the agencies. Currently the laws say what information governments *may* collect regarding national security 'with particular reference to', for example, serious crime and economic wellbeing but they need to say also what they may *not* collect, for example, information on lawful, peaceful political activities. Arguably, it is time for a statutory definition of 'national security'.

4.2 CSPs should be empowered to disclose the numbers of requests/orders for disclosure and number of users whose information is produced. It would still be against the law to reveal individual requests but a presumption of transparency is central to democratic security governance and this can only be rebutted if the efficacy of the programme would be substantially damaged if it were disclosed.[17]

4.3 Consider judicial rather than ministerial signing of warrants; this already exists with respect to some surveillance powers such as under the Police Act 1997, s.97 where prior authorisation by a (judicial) surveillance commissioner is required for intrusive police surveillance. If it is accepted that metadata is an intrusion on privacy equivalent to accessing content then the requirements for authorisation should be the same, whether that remains a minister or becomes a judge. Furthermore, RIPA (ss.21-25) empowers a wider range of 'public authorities' to request 'traffic data' and on more extensive grounds than national security.

4.4 GCHQ's code-breaking has always been directed against foreign governments and violent non-state actors but is now targeted also at companies. Tim Berners-Lee appears to speak for many in the software industry when he said that attacking commercial encryption was foolish because, once weakened, it would be easier for others to break. Therefore it contradicts the governments' fight against cybercrime and cyberwarfare and betrays the technology industry.[18] There is a clear need to re-think the adequacy of the general authorisation under ISA 3(1) (a) of what would otherwise be criminal activity and to explain government policy to the public.

4.5 In the light of these (and other) controversies concerning surveillance, the aim of any reconsideration of the legal framework must be to ensure:

---

[17] 'Vodafone takes a stand…' *Guardian* January 16, 2014, 2: Vodafone writing to UK ministers asking for right to disclose number of demands it receives for data. USG has just changed its policy so that the broad range of requests can be published, for example, January - June 2013, between 9,000-9999 Google user accounts were the subject FBI or FISA requests. *Reuters*, February 3, 2014.
[18] 'Father of the web condemns…' *Guardian*, November 7, 2013, 1-2.

a) increased certainty and clarity in the law. Primary legislation cannot be obfuscated on the grounds that it relates to 'national security' or 'sources and methods';

b) the effectiveness and propriety of agency policies and practices; and

c) improved public education.[19] Whatever the disposition of the law, there is a crucial political task for governments and intelligence oversight bodies to explain the limited *reality* of current security surveillance when the *potential* is clearly so vast and threatens public trust.

Peter Gill

Honorary Senior Research Fellow, University of Liverpool

[REDACTED]

6 February 2014

[19] On January 30, 2014 the Prime Minister said to the Select Committee on National Security: 'I do think politicians, police chiefs, the intelligence services have got a role in explaining what this is all about. Snowden inevitably raises questions about "who has access to my data and why"' 'PM: my failure to make case…' *Guardian* January 31, 2014, 8.