**Intelligence and Security Committee of Parliament**

**Privacy and Security Inquiry**

**7th February 2014**

This submission is from Professor Charles D. Raab, Professor of Government in the School of Social and Political Science, University of Edinburgh. My academic teaching and research has concerned privacy, processes involving personal information, surveillance, and the regulatory and governance arrangements that relate to these. I am not a specialist in the security and intelligence services, although some of my work on the above topics is relevant to their activities. I am writing in my personal capacity.

## Executive Summary

This submission is limited largely to addressing guidelines 6(a) and 6(b) of the Call for Evidence. It draws attention to ambiguities in the terms used: 'privacy', 'security', 'collective security', 'individual right', and 'balance'. It argues that clarity in the use of these terms is important in opening up new and more complex insights into what is at stake in the relationship between the security and intelligence services and the public, and in the performance of effective scrutiny and oversight. It considers that a better grounding is needed so that more nuanced criteria for judgment can be applied to these security and oversight tasks. It refers to some current proposals from the USA that might inspire comparable measures to place oversight on a better and more transparent basis, potentially leading to greater public confidence.

## Submission

1. I welcome the Intelligence and Security Committee's (ISC) attempt to broaden its inquiry into the legal framework for the interception of private communications. I would urge it to use its special knowledge of the formal internal organisation, procedures, and norms of intelligence agencies to widen its canvas in order to include inquiry into these extra-legal matters insofar as they might lead to the improvement of its scrutiny of the work of these agencies.

2. It is vitally important that the laws, administrative arrangements and normative cultures in this exceptionally difficult and sensitive field enjoy public confidence and. In a democracy, the public's support for legitimate state security and intelligence work is crucial, so that they see this work as being carried out in their interest and not as the operations of security services who regard citizens as suspicious potential agents of terror, crime and other threats to the state and society. However, these relationships between the citizen and the state may have been damaged especially by recent surveillance revelations and allegations emanating from the Snowden episode.[1] A significant proportion of public and informed opinion now registers doubts that the security services are sufficiently under control and are

[1] In the pre-Snowden era, the implications of surveillance, albeit not of national security, for citizens were investigated in *Surveillance: Citizens and the State*, House of Lords, Select Committee on the Constitution, 2nd Report of Session 2008-09, HL Paper 18.

operating within justifiable limits consonant with robust estimates of threats to national security and public safety.

3. These are questions of public perception that may not necessarily reflect the reality of how these services act and think, but perceptions are important and the services, as well as their overseers, must aim to dispel any unwarranted conceptions through as much transparency as possible. Public control and oversight through elected representatives and accountable appointees is an essential principle in a democracy, and can be a vehicle for transparency. The processes of independent scrutiny can play an essential part in reinforcing justifiable public support through investigation, questioning, and scepticism. Mediating between the public and the intelligence and security services, the ISC could play a vital part in helping to restore, or to establish, a high level of public confidence. It could do this through an enhanced role in making intelligence and security activities more transparent and accountable, consistent with the interests of effectiveness, and in exercising its judgment to criticise practices that have a negative effect on rights and liberties. In this judgment, the principles of necessity and proportionality should be applied rigorously and independently, and their application should be open, as far as possible, to interrogation and challenge at relevant stages of the security and intelligence activities concerned. This may be a matter for legislation, but also for the internal governance of agencies and for external scrutiny machinery. Transparency should be a main criterion for the improvement of present arrangements.

4. The Call for Evidence asks: 'What balance should be struck between the individual right to privacy and the collective right to security?' I believe this formulation of the issue is mistaken, rhetorical and imprecise; it impedes a deeper understanding of what is at stake for the individual, society and the state. Principles underlying the work of scrutiny, and judgments of the legitimacy of surveillance and security operations, would be better grounded if alternative ways of construing the relationship between security and privacy were understood and incorporated into practice. The following paragraphs examine this.

5. Three difficulties can be identified here. The first one is the way in which 'privacy' is construed. Privacy is indeed an individual right: fundamental but not absolute, and enshrined in prominent national and international legal instruments. However, privacy's importance goes beyond that of the individual, as is argued at the leading edge of academic and legal commentary. Privacy is acknowledged to be a crucial underpinning of interpersonal relationships, of society itself, and of the workings of democratic political systems.[2] To consider privacy only as an individual

[2] Among many other sources, see Solove, D. (2008) *Understanding Privacy*, Cambridge, MA: Harvard University Press; Regan, P. (1995) *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill, NC: University of North Carolina Press, ch. 8; Nissenbaum, H. (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford, CA: Stanford University Press; Goold, B. (2009) 'Surveillance and the Political Value of Privacy', *Amsterdam Law Forum* 1 (4), http://amsterdamlawforum.org; Cohen, J. (2012), *Configuring the Networked Self: Law, Code, and the Play of Everyday Life*, New Haven, CT: Yale University Press; Schoeman, F. (1992) *Privacy and Social Freedom*, Cambridge: Cambridge University Press; Steeves, V. (2009) 'Reclaiming the Social Value of Privacy', in Kerr, I., Steeves, V. and Lucock, C. (eds.), *Lessons From the Identity Trail: Privacy, Anonymity and Identity in a Networked Society*, New York, NY: Oxford University Press; Bennett, C. and Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective*, Cambridge, MA: MIT Press, ch. 2; Raab, C., (2012) 'Privacy, Social Values and the Public Interest', in Busch, A. and Hofmann, J. (eds.) 'Politik und die Regulierung von Information' ['Politics and the Regulation of Information'], *Politische Vierteljahresschrift* Sonderheft 46, Baden-Baden: Nomos

right is to ignore its value in these other dimensions, and thus to lose sight of its fuller significance in theory and practice. When individual privacy is protected, the fabric of society and the functioning of political processes and the exercise of important freedoms are thereby protected. When it is eroded, society and the polity are also harmed; it is in the public interest, and not only in the interest of the individual, to protect privacy. The individual right may be infringed for legal and legitimate reasons, such as the overriding importance of other rights and interests, but the claims of the latter to supervene must be argued and not merely asserted, must not be permanently accepted, and may ultimately be a matter for judicial determination. The unfortunate example of societies and of individuals under totalitarian or authoritarian governments serves as a reminder of the importance of these points.

6. The second difficulty lies in the common and repeated assumption made by politicians, the media, and the general public, that the issue is one of 'national security' *versus* 'personal privacy'. In practice, this assumption typically leads to the conclusion that this 'collective right' must normally trump the 'individual right' to which it is thought to be opposed. It is very difficult to counter this, especially in the present climate of fear. This is unfortunate, especially when the collective value of that individual right can also be seriously considered to be important, as explained above. The precedence taken by national security offers little scope for solutions that are more consistent with articulating the kind of society and polity we wish to sustain. Construing security and privacy as opposed also fails to recognise that both collective security and individual privacy are two expressions of a public interest, as argued above, and of the nature of the rights in question; this failure points up the facile nature of the supposed antagonism as a general principle.

7. A similar argument has been made about the relationship between security and liberty. A strong case can be supported for scepticism about whether seeing these values or rights as at odds is a proper way of looking at it.[3] In an atmosphere of fear of terrorist and other attacks, the conflictual way in which the relationship between security and liberty (or privacy) is presented has rhetorical force and supports arguments in favour of security practices and organisations far more than it does for liberty or privacy protection and the regulation of infringement. The interests that seek to perpetuate this predominance are stronger and louder than those who would challenge it and seek other kinds of reconciliation.

8. This is where independent organisations for regulation and scrutiny can play a crucial role in creating a level playing-field for the interests involved and in ensuring that there should be no presumption in favour of one side of the argument. But they can also play a crucial role in scepticism about whether the 'argument', if any, is correctly stated: that is, the claim that national security and privacy are antagonists, and that the former must prevail because of the way the 'collective' is construed. Where the old quips, 'better safe than sorry', 'there are no votes in privacy' and 'privacy is dead', are still recited in governmental and commercial sectors, it is important to have some means of offsetting the facile assumptions that often underlie policy and practice in the security field. Nor is it persuasive, on grounds of principle and rights, to claim glibly that 'the public doesn't care about privacy', as if the

---

Verlagsgesellschaft.

[3] See the critical and sceptical arguments in Waldron, J. (2003) 'Security and Liberty: The Image of Balance', *The Journal of Political Philosophy*, vol. 11, 191-210; Loader, I. and Walker, N. (2007) *Civilizing Security*, Cambridge University Press, 54-56.

exercise and validity of rights should depend on the state of public – even majority – opinion as ascertained in surveys, themselves difficult to interpret and often severely flawed.[4]

9. In this regard, it may be useful to draw inspiration from the recent report published by President Obama's Review Group on Intelligence and Communication Technologies,[5] a group established to determine how the protection of national security and respect for privacy and civil liberties can both be accomplished in the circumstances of intelligence operations following the Snowden revelations. Whilst the United States and the United Kingdom are considerably different in their governmental machinery and policy processes so that it would be difficult for the UK to transpose major structural innovations directly, the spirit and intent of the Review Group's recommendations command attention.

10. Two of its recommendations in particular are worth noting. Recommendation 26 calls for 'the creation of a privacy and civil liberties policy official located both in the National Security Staff and the Office of Management and Budget'. Separate from compliance, such an official would co-ordinate privacy policy within government, 'including issues within the intelligence community… [and] ensure that privacy issues are considered by policymakers.' The official would provide 'a focal point for outside experts, advocacy groups, industry, foreign governments, and others to inform the policy process.'[6] Whatever the machinery might be for giving effect to this idea in our country, having such a role performed at the centre of security policy-making, management and oversight would provide a counterweight to those interests that might undervalue the importance of privacy and civil liberties in their programmes and operations.

11. Recommendation 27 calls for a Civil Liberties and Privacy Protection Board to 'oversee Intelligence Community activities for foreign intelligence purposes, rather than only for counterterrorism purposes'. It would also 'be an authorized recipient for whistle-blower complaints related to privacy and civil liberties concerns from employees in the Intelligence Community'. Moreover, the creation of an Office of Technology Assessment within the Board is considered useful 'to assess Intelligence Community technology initiatives and support privacy-enhancing technologies'.[7] As the Report states, '[a]n improved technology assessment function is essential to informing policymakers about the range of options, both for collection and use of personal information, and also about the cost and effectiveness of privacy-enhancing technologies.'[8]

12. Inspired by these recommendations, innovations tailored to the circumstances of our government could provide important means for augmenting the UK's slender oversight and scrutiny machinery. They would create additional capacity and

[4] Public opinion surveys of attitudes towards privacy and security have been examined in the PRISMS project conducted under the European Union 7th Framework Programme, in which the author participates.

[5] *Liberty and Security in a Changing World*, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, 12 December 2013.

[6] Ibid., pp. 194-5.

[7] Ibid., p. 195. Privacy impact assessment (PIA) has become a widespread technique for information systems and technologies; see Wright, D. and De Hert, P. (eds.) (2012, *Privacy Impact Assessment*, Dordrecht: Springer. Among the organisations that conduct PIA is the USA's Department of Homeland Security; see https://www.dhs.gov/privacy-office-privacy-impact-assessments-pia.

[8] Ibid., p. 198.

functions with which government would not only be able to implement its concern for privacy and civil liberties in the midst of security processes, but also to be seen to be doing this in an open and accountable way. To be sure, this might entail constitutional changes in our system that have implications wider than those for the intelligence and security services alone. But, in part, they relate to guideline 6(b) of the ISC's Call for Evidence in dealing with the apparent need to review the legal framework in response to developments in information technology. They also resonate with guideline 6(a) by suggesting a way in which the claims of privacy protection could be more effectively represented in the highest counsels of government, and in which a wider policy-relevant discourse on privacy might be facilitated.

13. The third difficulty lies in the way 'security' is construed. As with privacy, there are many ways of understanding this – or its cognate, 'public safety' – and whatever right is considered to pertain to it, as well as its relationship to other rights.[9] Leaving aside the question of individual or personal security, one issue is that 'collective' security could refer to security at a variety of levels: for example, international, national, local, neighbourhood, or social group. How the claims of each of these might be promoted in the light of the right to privacy (itself of diverse meanings), and thus the nature of any reconciliation, will vary. Another issue is whether objective security – involving probabilities of risk – and/or subjective security – involving feelings of insecurity – should be at the focus of attention, and how these two foci can be reconciled.[10] A further issue is whether privacy and civil liberties (or freedoms) should not themselves be regarded, at least in some respects, as valuable because of the security and safety – not least, of personal data – they provide for individuals, groups and societies. If so, their relationship to each other is far more complex and cannot be glossed over by a rhetoric of the 'opposed' rights or values of security and privacy.[11] This observation is reflected in President Obama's Review Group's remark that '[t]he United States Government must protect, at once, two different forms of security: national security and personal privacy'.[12]

14. It follows that, if both privacy and security are contested and inter-related concepts, the idea that they can be 'balanced' or 'traded-off' must also come under sceptical scrutiny.[13] President Obama's Review Group noted that '[t]he idea of "balancing" has an important element of truth, but it is also inadequate and misleading'.[14] Whether 'balancing' is between one individual right and another, or

[9] See Zedner, L. (2009) *Security*, London: Routledge; Zedner, L. (2003) 'The Concept of Security: An Agenda for Comparative Analysis', *Legal Studies*, vol. 23, 153-175; Zedner, L. 'Seeking Security by Eroding Rights: The Side-stepping of Due Process', Fredman, S. 'The Positive Right to Security', and Lazarus, L. 'Mapping the Right to Security', all in Goold, B. and Lazarus, L. (eds.) (2007) *Security and Human Rights*, Oxford: Hart Publishing.

[10] Chandler, V. 'Privacy Versus National Security: Clarifying the Trade-off', in Kerr *et al.* (eds), op. cit.

[11] Raab, C. (2014), 'Privacy as a Security Value', in, Schartum, D. and Bygrave, L. and Bekken, A (eds.) *Jon Bing: En Hyllest / A Tribute*, Oslo: Gyldendal.

[12] *Liberty and Security in a Changing World*, op. cit., 14.

[13] See van Lieshout, M., Friedewald, M., Wright, D. and Gutwirth. S., (2013) 'Reconciling privacy and security', *Innovation – The European Journal of Social Science Research* vol. 26, nos. 1-2, 119-132. This is the focus of attention of the PRISMS project conducted under the European Union 7th Framework Programme, in which the author participates.

[14] *Liberty and Security in a Changing World*, op. cit, 16. The Panel nevertheless continues to use the term in developing its Recommendations. See also Dworkin, R. (1977) *Taking Rights Seriously*, London: Duckworth; Waldron, op. cit; Raab, C. (1999) 'From Balancing to Steering: New Directions

between an individual right and a collective right, or between an individual right and social or collective utility, also requires specification and precision if 'balancing' – even if inescapably built into our mindset – is to be taken away from the realm of shorthand and slogan.

15. In any case, the assumptions about equilibrium and about a supposed common metric for weighing are not clear and are doubtfully warranted. Is it suggested that we can know, and can all agree, how much (and whose) privacy should or should not outweigh how much (and whose) security? In addition, the proposal to engage in balancing is by itself silent about the method by which a balance can be determined and challenged, and about who is to determine it. Moreover, whether 'balance' refers to the method, or to its outcome, is often left unexplained by its proponents. The published decisions in legal cases are one source for understanding, and perhaps disputing, the weighing process and the arguments used, for instance about necessity and proportionality. It remains to be seen how these understandings can be disseminated in the much more closed conditions of the intelligence and security service where strategic and operational decisions have to be made, and also brought to bear in their oversight and scrutiny.

16. In conclusion, perhaps a better question for the Committee to ask would be: 'in combating terror and other threats, how can we ensure that, by applying more nuanced understanding, the claims for security measures are not the default when other values and rights are also at stake?' In carrying out their scrutiny, those who exercise regulatory and oversight functions must ascertain the purpose and effectiveness of security and intelligence service activities as well as their necessity, proportionality, legitimacy and legality. They must also press those services to show how they have justified their operations by means of these criteria, and have taken seriously the likely effect upon privacy and liberty construed as broadly as possible. They should also, and perhaps in the first instance, clarify and find means to widen the debate about the meaning of 'privacy', and especially of 'security' and 'national security'; and about how surveillance and intelligence activities affect the achievement of these objectives. This would help to move these terms, as well as security policy and practice, away from the realm of automatic acquiescence in invasive surveillance and towards constructive and critical public and parliamentary debate about the rights that are involved, yet consistently with the justifiable secrecy that surrounds strategy and operations. How transparency and secrecy can themselves be reconciled is in itself, of course, a matter for debate. But public confidence may be the ultimate beneficiary of all these processes of thinking and decision; in the long run, this confidence may be the most essential touchstone for security policy.

---

for Data Protection', in Bennett, C. and Grant, R. (eds.), *Visions of Privacy: Policy Approaches for the Digital Age*, Toronto: University of Toronto Press.