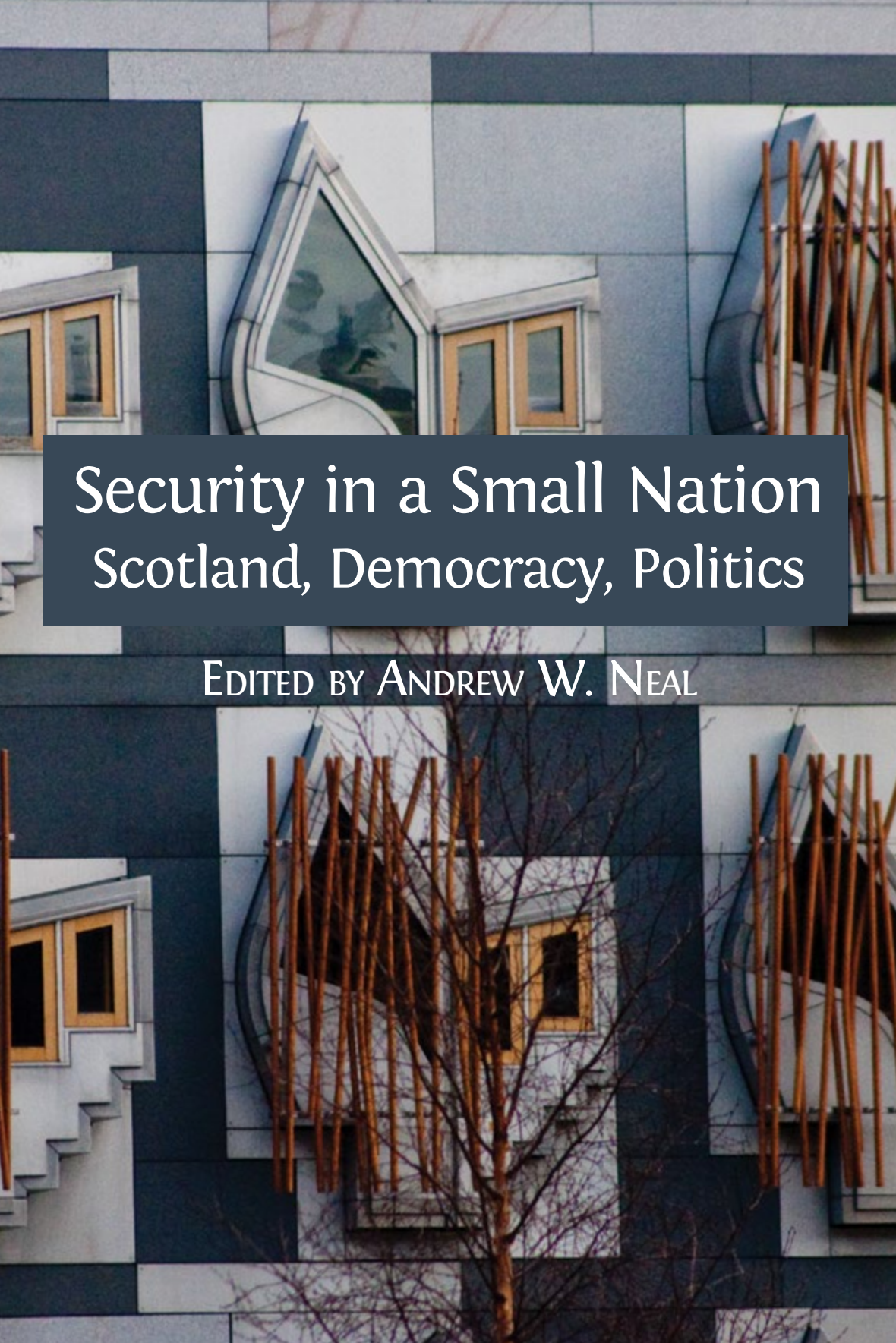


Security in a Small Nation
Scotland, Democracy, Politics

Edited by Andrew W. Neal

Security in a Small Nation

Scotland, Democracy, Politics

Edited by Andrew W. Neal
Centre for Security Research
University of Edinburgh

OpenBook Publishers

https://www.openbookpublishers.com

Open Reports Series, vol. 4 | ISSN: 2399-6668 (Print); 2399-6676 (Online)

ISBN Paperback: 978-1-78374-268-4
ISBN Hardback: 978-1-78374-269-1
ISBN Digital (PDF): 978-1-78374-270-7
ISBN Digital ebook (epub): 978-1-78374-271-4
ISBN Digital ebook (mobi): 978-1-78374-272-1
DOI: 10.11647/OBP.0078

Cover image: Scottish Parliament (2011) by deargdoom57, CC BY 2.0. Image from Flickr, https://www.flickr.com/photos/deargdoom57/5471878523/

All paper used by Open Book Publishers is SFI (Sustainable Forestry Initiative), PEFC (Programme for the Endorsement of Forest Certification Schemes) and Forest Stewardship Council(r)(FSC(r) certified.

Printed in the United Kingdom, United States, and Australia
by Lightning Source for Open Book Publishers (Cambridge, UK)

3. Security, Privacy and Oversight

Charles D. Raab

This chapter looks at conceptual and practical issues concerning 'privacy' and 'security' as they affect the oversight of security and intelligence services. It considers these issues in the light of three recent seminal reports in the UK and one in the US. Taking a critical view of the conventional wisdom surrounding the concepts of 'privacy' and 'security' and of the way the values they represent are thought to be reconcilable, this contribution argues that a better grasp of the relationship between these two areas in theory and practice is an important component of satisfactory oversight of intelligence activities. In addition, the extent to which overseers and other policy actors can keep abreast of technological developments is identified as a problem for the effectiveness of legislation and oversight, requiring changes to existing procedures.

https://doi.org/10.11647/OBP.0078.03

The long-awaited British debate on the extent to which the security and intelligence services are — and how they could be — effectively kept within the bounds of the rule of law and the workings of a healthy democracy gathered pace in 2015. Among the most prominent events in this period were the publication of three reports from a range of weighty participants and commentators: the Intelligence and Security Committee of Parliament (ISC); David Anderson QC, the Independent Reviewer of Terrorism Legislation (IPR); and the Royal United Services Institute (RUSI).[1] A controversial Draft Investigatory Powers Bill was introduced into Parliament in November 2015. It drew considerably upon Anderson's report especially, and travelled on a somewhat potholed pathway until it reached the statute book in November 2016.

In these post-Snowden times, the three reports have attracted much comment and criticism, but also — and to different extents — some praise for having moved the issue further into the public arena, and for having raised a range of questions for public and political debate. They also provide an insight into the way the issues are considered in the counsels of the state, and into the perceptions and (mis)conceptions that colour any attempt to deliberate on the problems and to move towards a better system of oversight of surveillance and intelligence activities. The reports bring a mixture of both stale and fresh air to one of the most crucial contemporary issues affecting the relationship between citizens and the state.[2] This chapter does not attempt to review in detail or to appraise the reports' recommendations and the commentary that they have spawned in traditional and social media, among interested parties, and in academia.

1 Intelligence and Security Committee of Parliament, *Privacy and Security: A Modern and Transparent Legal Framework* (London: HMSO, 2015), https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt(web).pdf; David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (London: HMSO, 2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf; Royal United Services Institute for Defence and Security Studies, *A Democratic Licence to Operate: Report of the Independent Surveillance Review* (London: Royal United Services Institute for Defence and Security Studies, 2015).

2 See an earlier investigation into this subject: House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State, 2nd Report of Session 2008–09, Hl Paper 18-I* (London: HMSO, 2009), http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm. This did not, however, deal centrally with national security and intelligence.

Others have described and assessed the ISC and other oversight bodies in terms of their historical origins, and the remits, expectations, and positions within the constitutional orders of their political systems. Their strengths, but especially their deficiencies, in providing satisfactory oversight and in holding intelligence services to account have been at the forefront of scholarly attention.[3] Somewhat less discussed is the relationship between intelligence, oversight, and human rights, although this has also been critically explored in recent years with regard to the UK.[4] The chapter therefore focuses on these areas that need deeper consideration and re-thinking, and looks across the Atlantic for some of the illumination of practices and concepts that is required if oversight is to be improved in the country. In particular, it brings into view some underlying conceptual issues that have been overlooked both by commentators and oversight practitioners. The way in which under-specified notions of privacy, security, and balance might be more fully and soundly articulated is central to this discussion. These matters bear upon the processes and institutions of oversight, and on the rights-related assumptions that are entailed when intelligence agencies and overseers consider the necessity of limiting surveillance.

Although this chapter does not examine or comment on the Investigatory Powers Act, the latter applies to Scotland with, it appears, mainly *mutatis mutandis* variations that take account of Scottish institutional and jurisdictional dimensions, such as the implementation of interception warrants and other differences.[5] It should be pointed out

3 See, for example, Mark Phythian, 'The British Experience with Intelligence Accountability', *Intelligence and National Security*, 22, 1 (2007), 75–99; Andrew Defty, 'Educating Parliamentarians About Intelligence: The Role of the British Intelligence and Security Committee', *Parliamentary Affairs*, 61, 4 (2008), 621–41; L. E. Halchin and F. Kaiser, *Congressional Oversight of Intelligence: Current Structure and Alternatives* (Washington, DC: Congressional Research Service, 2012); Samuel J. Rascoff, 'Presidential Intelligence', *Harvard Law Review*, 129, 3 (2016), 633–717.

4 See, for example, Peter Gill, 'The Intelligence and Security Committee and the Challenge of Security Networks', *Review of International Studies*, 35, 4 (2009), 929–41; Peter Gill, 'Intelligence, Threat, Risk and the Challenge of Oversight', *Intelligence and National Security*, 27, 2 (2012), 206–22; Ian Leigh, 'Rebalancing Rights and National Security: Reforming UK Intelligence Oversight a Decade after 9/11', *Intelligence and National Security*, 27, 5 (2012), 722–38; Peter Gill, 'Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the "War on Terror"', *Intelligence and National Security*, 22, 1 (2007), 14–37.

5 See, for example, sections 21, 22, 30, 39, 117, 118 and 125 of the Act. Note that members of the Scottish Government, and not only Scottish Ministers in the UK Government, may be involved in warrantry processes.

that most statutory law in this area covers the UK as a whole, although Scotland has a separate Regulation of Investigatory Powers Act, and the machinery of oversight is likewise unified. Similarly, in terms of the focus of this chapter on concepts of privacy and security, there is currently no significant Scottish angle that would affect the intelligence matters under consideration, at least in terms of the way data protection (which is not the same as privacy, but is closely related to it) is enshrined in law and implemented through regulatory machinery.[6] In areas that are perhaps parallel to the data protection regime but arguably not directly relevant to the proposed investigatory powers legislation, there are some Scottish differences that have at times come into the limelight: for instance, a shorter period for the retention of DNA data in law enforcement.[7] Possibly more significantly for future challenges brought on transparency grounds, Scotland has a separate Freedom of Information Act that has its own Commissioner and judicial regime capable of deciding matters differently. Whilst it is not clear that these variations will have a bearing on any oversight and adjudication of the Act, future constitutional scenarios for the UK could entertain questions about whether an independent Scotland, for example, might have the scope to develop a different understanding of security and privacy to underpin different legislative provisions for security, and for oversight arrangements.

The question of oversight

In addition to conceptual issues, the performance of oversight requires further inquiry, partly in terms of the outlooks that shape it, but also in terms of machinery and process. Institutions, processes, and incisive interrogation are intertwined aspects of oversight. Effectiveness has partly to do with the structures and mechanisms that are put in place to hold the intelligence and security services accountable. The degree of independence of this machinery might well shape the ability of overseers

6 As will be mentioned in a later section, data protection concerns the privacy of personal data, but there are many other domains in which privacy might be at stake.

7 This was regarded favourably in the European Court of Human Rights decision in the case of *S. and Marper v. The United Kingdom* (Applications nos. 30562/04 and 30566/04), 4 December 2008.

to ask the right questions, and hence put limits to the effectiveness of their oversight. The capacity to ask the right questions is also related to the conceptions, assumptions and thinking that underlie them; and this, in turn, owes much to the individuals, personalities, and backgrounds that are represented in these structures. This intertwining is not quite circular, but tendencies to closure in the oversight 'club' are strong, given — for all its internal diversity and scope for dissensus — the tightly-knit nature of the security, intelligence, defence, and foreign-policy community that presides over the channels of oversight and accountability, and thus arbitrates the intellectual basis of oversight (see Chapter 7 for a discussion of this community and its relationship to the wider field of politics). Schattschneider long ago observed famously that '[s]ome issues are organized into politics while others are organized out': an institutional 'mobilization of bias' that leaves many issues and alternative perspectives out of account, or suppresses them.[8] The understandable need for opacity and the near-closure of the oversight process abets this bias, and also militates against the prospects for wider and better-informed debate about national security throughout society and the political system. In the absence of dramatic events (e.g., the Snowden revelations) triggering convulsions of public and political opinion, leading to some embarrassment in the intelligence and oversight community, demands for greater transparency are easily defeated, ostensibly for good reasons, thus further deepening public scepticism and lack of trust in government and politics.[9] This is a predicament for which there are no clear solutions, especially at a time when such scepticism and even revulsion is at a high level.

The intelligence and security services are bound by a sense of mission: our continued safety and security is the paramount rationale for their role and their claim on the material and governmental resources of the country. *How* safe and secure we, and the country, need to be kept is never explained or debated: 'safety' and 'security' enjoy the status of ineffability.

8 Elmer E. Schattschneider, *The Semisovereign People: A Realist's View of Democracy in America* (New York: Holt, Rinehart and Winston, 1960), p. 71; This can be seen as an exercise of power, see Steven Lukes, *Power: A Radical View* (Basingstoke and New York: Palgrave Macmillan, 2004).

9 On scepticism, see Mark Phythian, 'Still a Matter of Trust: Post–9/11 British Intelligence and Political Culture', *International Journal of Intelligence and CounterIntelligence*, 18, 4 (2005), 653–81.

In fulfilling their mission, the services are circumscribed by the rule of law and by specific regulations that include certain practices and exclude others, and they are bound to respect privacy and other rights. Whether the rule of law is maintained in the intelligence and security process has to do in part with the way in which these services understand the effects of their performance upon individuals and society, with respect to the values of security (or safety), privacy, and the exercise of freedoms, and bring this understanding to bear on their operations.

The oversight machinery's enquiry into these matters is therefore aimed at ensuring not only the effectiveness of these services but also their adherence to constitutional and legal circumscription. As agents in an accountability process, overseers should be able to require that the services give accounts — stories about the performance of their role — but should also be able and willing to interrogate those accounts, probing them for evidence and explanation, and perhaps challenging them with alternative constructions of the stories and different ways of thinking about the values that are served by security activity.[10] By itself, the statutory framework for oversight of the services cannot tell one about the effectiveness of oversight in practice, which — as already been indicated — has a great deal to do with the way oversight roles and powers are exercised and the way the machinery of oversight is constituted and populated. These latter factors, in turn, affect the way in which overseers think about what they are doing, and upon their understanding of the values at stake when the intelligence and security services perform their work. Oversight depends upon the enquiry to which the intelligence and security services are, or will be, subject when they undergo scrutiny, by the way the questions are shaped by conceptual understandings and frameworks, and by the parameters that are set in the oversight process.

There is a second and consequential step in this process. Overseers are intermediaries who act on behalf of the general public or its parliamentary representatives, but oversight bodies are themselves

10 In a related field, see C. Raab, 'The Meaning of "Accountability" in the Information Privacy Context', in D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland and H. Postigo (eds.), *Managing Privacy through Accountability* (London: Palgrave Macmillan, 2012), pp. 15–32.

accountable to the latter for their performance of this role, and thus for the way they have held the intelligence and security services to account. Here, too, there are dilemmas about transparency, and a necessary element of trust that the public or Parliament must have in the veracity of the accounts that these intermediaries give, and in their effective performance of the oversight stewardship role. How the public or Parliament is able to interrogate the *overseers'* accounts, or to challenge them, is a conundrum that mirrors, at this level, that of the intermediaries' primary relationship to the intelligence and security services. Regarding both the security or intelligence services and the oversight bodies, this is not precisely the problem indicated by the frequently asked question, *quis custodiet ipsos custodes?* (who watches the watchmen?), for the buck does stop somewhere in the constitutional and practical make-up of parliamentary democracy (see Bochel and Defty in Chapter 3 for further discussion). It rather concerns how the guardians at both levels do their work, and how they frame and act out their 'take' on the values that underpin the work they carry out.

There are many dimensions of the vexed question of how, in a democracy, security and intelligence organisations, including law-enforcement agencies, can be subject to effective and transparent oversight procedures. The three reports mentioned above all cast light upon the current state of the art, and make many recommendations across a very wide range. There is no space here to look at any of these in depth; however, some important facets can be highlighted, upon which the conceptual, ethical and legal aspects of this chapter have some bearing. Oversight should be independent of the agencies and of the government. The importance of this autonomy, and the importance of the separate assessment of technologies, and of legal and ethical compliance, lies, in part, in the ability of independent overseers and assessors to ask questions that would probably not be asked from within the culture that prevails among security and intelligence officials. It is also necessary that the overseers should have sufficient technical knowledge to be able to relate those facts to values. Some of those questions might not only be about privacy and civil liberties, but also about the means and ends of security; and they might even enable fresh perspectives to be taken on just what constitutes privacy, security, risk and harm.

Understanding security and privacy

One of the main high-profile public issues in the work of intelligence and security services — and indeed in policing as well — is the extent to which their operations pay due regard to the liberties and rights of individuals and groups who may be affected by the covert or overt collection and use of personal information in the course of performing security-related intelligence work. This is not a question of malevolence or turning a blind eye to soft values by a hard-boiled professional culture, but one of cognition: how the services understand the wider world beyond the operation or tasks that they are called upon to perform, and how they bring to bear criteria of success or effectiveness that lie further afield than the achievement of specific objectives. Liberties, rights and the nature of security are topics and ideals that are difficult enough for philosophers, lawyers and other academic specialists to grapple with, let alone those who have to take them into consideration in the heat of their working day, and then to give an account of how they brought this thorny bundle to bear upon their activities. But the same goes for the overseers, who evaluate what is done by the overseen. For the participants in both parts of the oversight 'two-step', how the ostensibly competing imperatives — security, and rights and liberties — are to be reconciled is a perennial dilemma. It cannot be answered by formulaic methods or rhetoric, but must be considered in each instance, or class of instances, in which such competition is felt to arise, in the light of a more general clarification of the underlying principles that guide the application of these values in practice.

A relevant illustrative case in point where this reconciliation and a search for new approaches is attempted is the investigation that the ISC, the Intelligence and Security Committee of Parliament, launched into security and privacy with a call for evidence in December 2013. This was only a few months after the Snowden revelations of the mass surveillance activities of the US's National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ) had caused considerable reaction in political circles, in the media, and among concerned interest groups in the UK, the US, and around the world. The ISC announced that it was 'broadening its inquiry into the laws which govern the intelligence agencies' ability to intercept private communication. In addition to considering whether the current

statutory framework governing access to private communications remains adequate, the Committee is also considering the appropriate balance between our individual right to privacy and our collective right to security'.[11] The ISC's subsequent report held fast to this framing of the way it saw privacy and security. It did not elaborate upon what 'security' might mean. It never considered that the privacy of the individual, and the value of privacy, might be about more than just the individual and the value to her of the right of privacy, and it did not question the nature of the process of achieving 'balance'.

For the Government's part, Philip Hammond, the then UK Foreign Secretary, echoed the ISC's outlook in saying:

> We are after all, all of us in our private lives, individuals who seek privacy for ourselves and our families, as well as citizens who demand protection by our government from those who would harm us. So we are right to question the powers required by our agencies — and particularly by GCHQ — to monitor private communications in order to do their job. But we should not lose sight of the vital balancing act between the privacy we desire and the security we need.[12]

Note that it is as 'individuals' that we are said to seek privacy, but as 'citizens' we demand protection from harm; it is 'the privacy we desire' *versus* 'the security we need'. The rhetorical effect of these associations and contrasts would be quite different if they were reversed in each part of the statement; moreover, a 'balancing act' is asserted in describing the relationship.

We might be able to escape these deep-seated ritual constructions in our search for the best way to frame the guiding principles underpinning the work of oversight and accountability. If the ISC, and ministers or other government actors in their oversight roles, are to exercise their functions, they need to examine the assumptions that underpin these functions, and they need sometimes to ask awkward questions. How well equipped they are to do this, by virtue of their constitutional

11 Intelligence and Security Committee of Parliament, 'Privacy and Security Inquiry — Call for Evidence' (11 December 2013), https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20131211_ISC_Call_for_papers-Privacy.pdf

12 Foreign and Commonwealth Office and The Rt Hon Philip Hammond, 'Foreign Secretary Intelligence and Security Speech', Gov.uk, 15 March 2015, https://www.gov.uk/government/speeches/foreign-secretary-intelligence-and-security-speech

position, composition (in the case of agencies), resources and remit, is at issue. Moreover, the assumptions that form their mindset need to be articulated and subject to public discourse and debate.

Let us look at these issues. The first one lies in the way 'security' is construed. There are many ways of understanding 'security' — or its fellow, 'public safety'[13] — and whatever right is considered to pertain to it, as well as its relationship to other rights.[14] 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. Directly or indirectly, the intelligence and security services' activities involve all of these. How the demands for security at each of these levels might be promoted in the presence 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 in security activities and in their oversight (for example, in judging necessity and proportionality), and how these two perspectives can be reconciled.[15]

13 The distinction between 'security' and 'safety' is blurred, and their usage often interchangeable. Philip Hammond used the words 'safe' and 'safety' eleven times and 'security' eighteen times in his RUSI speech of 10 March 2015 on Intelligence and Security; Foreign and Commonwealth Office and The Rt Hon Philip Hammond (2015). Both the UK Conservative Party and Labour Party 2015 election manifestoes used 'safe', 'secure', and derivative words profusely and indiscriminately in relation to an enormous variety of issues: banking, borders, children, communities, the country, cyber activity, cycling, the economy, the elderly, energy supplies, families, farming, the Green Belt, health care, hospitals, jobs, the Middle East, neighbourhoods, religious practice, retirement, work, etc.

14 See Lucia Zedner, 'The Concept of Security: An Agenda for Comparative Analysis', *Legal Studies*, 23, 1 (2003), 153–75; Lucia Zedner, 'Seeking Security by Eroding Human Rights: The Side-Stepping of Due Process', in *Security and Human Rights*, ed. by Benjamin J. Goold and Liora Lazarus (Oxford: Hart, 2007), pp. 257–77; Lucia Zedner, *Security: Key Ideas in Criminology Series* (London and New York: Routledge 2009); S. Fredman, 'The Positive Right to Security', in *Security and Human Rights*, ed. by B. J. Goold and Liora Lazarus (Oxford: Hart, 2007), pp. 307–24; L. Lazarus, 'Mapping the Right to Security', in *Security and Human Rights*, ed. by B. J. Goold and Liora Lazarus (Oxford: Hart, 2007), pp. 325–46.

15 Jennifer Chandler, 'Privacy Versus National Security: Clarifying the Trade-Off', in *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, ed. by I. R. Kerr, V. M. Steeves, and C. Lucock (Oxford: Oxford University Press, 2009), pp. 121–38.

The second issue is the way in which 'privacy' is construed. Privacy as a fundamental but not absolute right is enshrined in prominent national and international legal instruments. However, privacy's importance goes beyond that of the individual: it is a crucial underpinning of interpersonal relationships, of society itself and its groups and categories of persons, and of the workings of democratic political systems. Although defining 'privacy' has long been highly contentious,[16] the trans-individual meaning and its implications for rights and freedoms is gaining ground in academic commentary[17] and is appreciated in constitutional argument and judicial decision as well as in some prominent reports. To consider privacy only as an individual right — or as a mere 'desire' — is to slight its fuller significance in theory and practice. When individual privacy is protected, the fabric of society, as well as 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 have privacy protected as a 'constitutive public good': a societal good, understood as an integral and essential element of society itself.[18] In that sense, we *need* privacy as *citizens*, and not just as customers or consumers of goods and services in the commercial marketplace.

16 See Ferdinand David Schoeman, *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press, 1984), p. 444.

17 Sources include Daniel J. Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008); Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: University of North Carolina Press, 1995); Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2009); Benjamin J. Goold, 'Surveillance and the Political Value of Privacy', *Amsterdam Law Forum*, 1 (2008), 3–6; Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale: Yale University Press, 2012); Ferdinand David Schoeman, *Privacy and Social Freedom* (Cambridge: Cambridge University Press, 1992); V. Steeves, 'Reclaiming the Social Value of Privacy', in *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, ed. by I. R. Kerr, V. M. Steeves, and C. Lucock (New York: Oxford University Press, 2009); Colin Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge, MA: MIT Press, 2006), Chapter 2; Charles Raab, 'Privacy, Social Values and the Public Interest', in *Politik Und Die Regulierung Von Information*, ed. by A. Busch and J. Hofmann (Baden-Baden: Nomos, 2012), pp. 129–51.

18 Ian Loader and Neil Walker, *Civilizing Security* (Cambridge: Cambridge University Press, 2007), p. 145.

In stark contrast, there is the assertion that 'the provision of basic security is the paramount human good, upon which all other political goods depend'.[19] Whilst the individual's right may be set aside for legal and legitimate reasons, such as the overriding importance of other rights and interests, including security, the claims of the latter to prevail must be argued — as it certainly can be, in given instances — and not merely asserted. However, they must not be permanently accepted by default, and may ultimately be a matter for the courts to determine in terms of necessity and proportionality. Insofar as these claims may be made on behalf of organisations whose legitimacy lies in their acting in support of 'collective' interests, to ignore the perception that privacy is *also* a collective citizen interest is to put a thumb on the 'balancing' scale. It is also powerfully to shape the public understanding of what is at stake by relegating the social and political value of privacy to the status of a claim that need not be seriously respected. Moreover — although this point cannot be discussed further here[20] — just as there are many dimensions and levels of security, *information* privacy, which was prominently at stake in mass surveillance of the kind illuminated by the Snowden revelations that instigated the inquiries and reports, is only one kind of privacy; privacy (e.g., of the body or of space) is often invaded even if information is not collected and processed further, including its communication through myriad channels.

The third issue concerns the relationship between security and privacy, and their reconciliation or 'balancing'. The ISC's view of the 'balance' or trade-off between individual privacy — and, indeed, other individual rights and liberties — and national security was neither inescapable nor unbiased in terms of what the implicit outcome should

19 Amitai Etzioni, *Security First: For a Muscular, Moral Foreign Policy* (Yale: Yale University Press, 2008), p. xviii.

20 See Rachel L. Finn, David Wright, and Michael Friedewald, 'Seven Types of Privacy', in *European Data Protection: Coming of Age*, ed. by Serge Gutwirth *et al.* (Dordrecht: Springer Netherlands, 2013), pp. 3–32; David Wright and Charles Raab, 'Privacy Principles, Risks and Harms', *International Review of Law, Computers & Technology*, 28, 3 (2014), 277–98; The latter article points to a further issue requiring exploration: the non-privacy effects of surveillance on individuals, groups and categories, which could be very important in the context of intelligence and oversight. See the discussion of harms of intelligence collection to 'vital interests' in Ross Bellaby, 'What's the Harm? The Ethics of Intelligence Collection', *Intelligence and National Security*, 27, 1 (2012), 93–117.

be.[21] In contrast, in another context — that of cyber security — the President of Estonia said: 'freedom and security need not contradict each other: secure online interactions, enabled by a secure online identity, is a precondition for full internet freedom'.[22] This is the beginning of a departure from conventional wisdom. The report by RUSI clearly staked out the ground for a fresh departure by casting doubt on the existing terms of public debate:

> The most striking characteristic of public discussions on surveillance to date is the perceived dichotomy between the rights or values of collective security and privacy. A common and repeated assumption made by politicians, the media and the general public is that these values are opposed, and that the issue is one of 'national security' versus 'personal privacy'. The subsequent assumption is that a trade-off can be made between the two: Is the right balance being struck between national security and civil liberties, or between collective security on the one side and individual freedoms and personal security on the other?[23]

Another step, perhaps more paradoxically, is to reflect on 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. As do national security strategies, they can involve protective, precautionary, defensive and risk-averse measures taken in the face of technologically assisted policy initiatives. In societies driven

21 See analogously Jeremy Waldron, 'Security and Liberty: The Image of Balance', *Journal of Political Philosophy*, 11, 2 (2003), 191–210; Chandler (2009); Charles Raab, 'From Balancing to Steering: New Directions for Data Protection', in *Visions of Privacy: Policy Choices for the Digital Age*, ed. by C. Bennett and R. Grant (Toronto: University of Toronto Press, 1999), pp. 68–93; Relevant arguments on privacy and security in the context of democracy are developed in Annabelle Lever, *Democracy, Privacy and Security* (Rochester: Social Science Research Network, 2015).

22 Toomas Hendrik Ilves, '"Rebooting Trust? Freedom *vs* Security in Cyberspace" Opening Address at Munich Security Conference Cyber', Office of the President, Republic of Estonia (Munich, 31 January 2014), https://vp2006-2016.president.ee/en/official-duties/speeches/9796-qrebooting-trust-freedom-vs-security-in-cyberspaceq. Office of the President, Republic of Estonia (Munich, 31 January 2014

23 Royal United Services Institute for Defence and Security Studies (2015), p. 216. These remarks underline points made in the author's evidence to the ISC inquiry and to Anderson. See Independent Reviewer of Terrorism Legislation, *Investigatory Powers Review Written Submissions (H-V)* (London: Independent Reviewer of Terrorism Legislation, 2015), https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/Submissions-H-Z.pdf

by counter-terrorism, law enforcement, and a preoccupation with personal safety, ever-increasing volumes and granularity of personal data are collected, mined, shared and stored in the name of security and safety. In those circumstances, privacy can provide a secure refuge for individuals and groups against the prying eyes of the state or private companies, whether that refuge serves inward-looking individual purposes or the possibility of external sociality and participation. To be secure in our homes is, at the same time, to inhabit a protected private space: one of the meanings of privacy. If so, the overlapping or even isomorphic relationship between privacy and security is far more subtle than might be imagined, and cannot be glossed over by a rhetoric of the 'opposed' rights or values of security and privacy.[24] The unfortunate example of societies under totalitarian or authoritarian governments, in which surveillance affords neither privacy nor personal security at the level of persons and groups, serves as a reminder of the importance of this point.

The affinity between privacy and security has begun to be appreciated in various quarters, such as the US, where the Review Group on Intelligence and Communications Technologies, appointed by President Obama, reported in December 2013.[25] In a section on Principles, the Review Group Report included the following:

> 1. The United States Government must protect, at once, two different forms of security: national security and personal privacy.
>
> In the American tradition, the word 'security' has had multiple meanings. In contemporary parlance, it often refers to national security or homeland security. One of the government's most fundamental responsibilities is to protect this form of security, broadly understood. At the same time, the idea of security refers to a quite different and equally fundamental value, captured in the Fourth Amendment to the United States Constitution: 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated […]'. Both forms of security must be protected.[26]

24 Charles Raab, 'Privacy as a Security Value', in *Jon Bing: En Hyllest/A Tribute*, ed. by D. W. Schartum, L. Bygrave, and A. G. B. Bekken (Oslo: Gyldendal, 2014), pp. 39–58.

25 The President's Review Group on Intelligence and Communications Technologies, *The NSA Report: Liberty and Security in a Changing World* (Princeton and Oxford: Princeton University Press, 2014).

26 *The NSA Report*, pp. 14–15.

In seeing that privacy itself has security value,[27] the Review Group Report subtly shifted the terms of policy and debate in a way that is available to other policy deliberations outside the specifically American constitutional context. This construction, of course, does not by itself necessarily undermine the idea that conflict may occur between collective and individual meanings of security. But by considering afresh the connection between privacy and security, it throws into question — on both the level of policy discourse and rhetoric, and on the legal level — the implicitly unequal weighting between these two desirable values. This inequality would most likely be reflected in the outcome of any attempt to 'balance' the two in a construction that pits the national interest against that of the individual. This may especially be the case in the climate of fear and vulnerability brought about by terrorism and other real or perceived attacks.[28] Individual rights have historically been set aside, albeit temporarily, in favour of collective ones or in favour of collective anxieties that construe national sovereignty and territorial integrity to be severely threatened. The Review Group Report was indeed explicit and sceptical about the question of 'balancing':

> 3. The idea of 'balancing' has an important element of truth, but it is also inadequate and misleading. It is tempting to suggest that the underlying goal is to achieve the right 'balance' between the two forms of security. The suggestion has an important element of truth. But some safeguards are not subject to balancing at all. In a free society, public officials should never engage in surveillance in order to punish their political enemies; to restrict freedom of speech or religion; to suppress legitimate criticism and dissent; to help their preferred companies or industries; to provide domestic companies with an unfair competitive advantage; or to benefit or burden members of groups defined in terms of religion, ethnicity, race, and gender.[29]

27 See Raab (2014).

28 Gill observes: 'The pressures on intelligence agencies to "deliver results" and on parliamentary and other oversight bodies to relax oversight are greatest when security fears and uncertainties are at their height. This is the danger of the oft-quoted need to "balance" security and rights; the need for oversight is actually greater at times such as this in order to promote effectiveness and prevent abuses of human rights' (Gill (2009), p. 221). He also asserts that 'intelligence can advance human security but the role of oversight remains to ensure that intelligence is conducted proportionately, not to seek some mythical "balance" between rights and security' (*ibid*, p. 218).

29 *The NSA Report*, p. 16.

Further evidence that supports the argument that the relationship between security and privacy (or other liberties) is complex can be found in US legislation: the Implementing Recommendations of the 9/11 Commission Act of 2007, which established a reconstituted Privacy and Civil Liberties Oversight Board (PCLOB) as an independent body in the Executive Branch.[30] On the one hand, Title VIII of the Act remained within a 'balancing' framework, charging the PCLOB to: 'analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties'.[31] On the other hand, it preceded this with a quotation from the National Commission on Terrorist Attacks Upon the United States' *9/11 Report* which, it said, had:

> correctly concluded that 'The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend'.[32]

The RUSI report's construction of the relationship between privacy and the values of democracy resembled this in spirit, and was markedly different from what the ISC (or former Foreign Secretary Hammond) presumed. Recognising the trans-individual importance of privacy to the nation's political and governmental practice, as well as to freedom of the press, it said:

> Privacy is an essential prerequisite to the exercise of individual freedom, and its erosion weakens the constitutional foundations on which democracy and good governance have traditionally been based in this country. […] Privacy is also a pre-requisite for democracy. It gives people the freedom that is needed to be personally autonomous, to seek out alternative sources of information and to question the status quo. […]

30 US Congress, *Public Law 110–53, 110th Congress—Aug. 3, 2007: Implementing Recommendations of the 9/11 Commission Act of 2007* (Congress.gov, 2007), https://www.congress.gov/bill/110th-congress/house-bill/1; For further discussion and background, see Garrett Hatch, 'Report for Congress Privacy and Civil Liberties Oversight Board: New Independent Agency Status' (Washington DC, 2012).

31 *Public Law 110–53*, p. 121 Stat. 352.

32 *Ibid.*; The quotation is from National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (Authorized Edition)* (New York: W. W. Norton & Company, 2011), p. 395.

> Those who challenge the state — through journalism or legal advocacy, for example — need to be confident they are not spied upon, otherwise they cannot do their jobs effectively, and such jobs are an acknowledged part of a functioning democracy.[33]

This report did use the term 'balance' in referring to various rights, but it immediately veered away from this trope; its understanding of rights was carefully phrased to reflect a sense of their deeper and more intricate mutual dependence:

> The concepts of liberty, security and privacy are central to a number of universal rights outlined by important pieces of twentieth-century treaties and legislation […] These rights are not seen as absolute or unconditional, but rather as qualified rights. This qualification — that these rights are in turn subject to other rights — is important if these rights are to be consistent, balanced and mutually reinforcing. Each right must be protected and respected, to the greatest extent possible, but it cannot exist in isolation. There is no privacy without respect for security; there is no liberty without respect for privacy; security requires both certain liberties and privacy. It is therefore unfruitful (indeed misleading) to cast debates about privacy, liberty and security as a matter of choice or 'balancing' between these rights, still less to think of trade-offs between these rights.[34]

Furthermore, RUSI said:

> The relationship between privacy on the one hand, and liberty and security on the other, is complex. Discussions of privacy and security are often described as a matter of finding or striking a 'balance'; this traditional metaphor can be misleading. There is no metric for 'weighing' different rights, or even for comparing the 'weight' of different rights in particular cases. But it is feasible to set out robust standards that must be met in adjusting rights to one another and to devise and establish structures to do so.[35]

Anderson devoted a chapter to exploring the meaning and functions of 'privacy', showing an understanding of the literature as well as the case law that underscored the multifaceted and contextual nature of the concept, its values to the individual and society, its relation to other

33 Royal United Services Institute for Defence and Security Studies (2015), pp. ix, 2.10.
34 *Ibid.*, p. 2.3.
35 *Ibid.*, p. 2.6; see also the author's evidence to the ISC inquiry: Independent Reviewer of Terrorism Legislation (2015).

rights and freedoms, and its practical manifestations. For example, the report cited case law in highlighting the importance of privacy:

> A good start is provided by the recent judicial description of privacy protection as 'a prerequisite to individual security, self-fulfilment and autonomy as well as to the maintenance of a thriving democratic society'. As that statement implies, the privacy ecosystem has individual, social and political aspects.[36]

The Anderson report clearly grasped the subtlety of privacy's importance beyond the individual. Although it did use the terms 'balance' and 'balancing' in a more or less conventional way, this was done frequently in a legal framework to show the relevance of the test of *proportionality* that is applied in judicial decision-making and is urged as a principle for political and organisational decision contexts as well. Thus proportionality under Article 8(2) of the European Convention on Human Rights (ECHR) — the 'right to privacy' — 'is determined via a balancing exercise, which may for example require "*the interest of the […] state in protecting its national security*" to be balanced against "*the seriousness of the interference with the applicant's right to respect for his private life*"'.[37]

This construction invites a more nuanced resolution of the reconciliation — or, indeed, the 'balancing' — of the two values or rights in circumstances where national security is implicated. It shares something of the spirit of the US's Review Group Report, which, like Anderson, discussed the matter within a framework of principles, here putting it in terms of risk, and extending the list of consequences

36 Anderson cites the Canadian Supreme Court case of *R v. Spencer*, 2014 SCC 43, involving privacy and anonymity on the Internet and the 'reasonable expectation of privacy'; *A Question of Trust*, p. 27. See Barry Sookman, 'Internet Users' Privacy and Anonymity Protected by Supreme Court: *R v. Spencer*', 13 June 2014, http://www.barrysookman.com/2014/06/13/internet-users-privacy-and-anonymity-protected-by-supreme-court-r-v-spencer/ Anderson cited the Court's differentiation of several types of privacy interest and meaning. Nevertheless, the public's feeling of safety and security may justify the necessary and proportionate overriding of privacy in justifiable circumstances: see *A Question of Trust*, p. 40.

37 Anderson quotes the case of *Leander v. Sweden*, para. 59; emphasis in original: *ibid.*, p. 76. See also *ibid.*, p. 252: 'Central to most of these rights are the concepts of necessity and proportionality. Because those concepts as developed by the courts are adaptable, nuanced and context-specific, they are well adapted to balancing the competing imperatives of privacy and security'. The ISC Report also emphasised the importance of the test of proportionality.

beyond the risk to national security to embrace privacy, civil liberties, international relations, and international commerce.[38]

Policy, oversight and technology

In the US, there has been a long saga regarding the establishment of ancillary machinery for security and intelligence policy and practice.[39] The PCLOB was eventually constituted in 2012 as an independent agency in the Executive Branch, but the independence of such a body had been a matter of contention over the previous eight years. So too have been PLCOB's remit, powers and composition; such arguments continue, with the Review Group Report's recommendation that this body should be supplanted by a Civil Liberties and Privacy Protection (CLPP) Board that would have foreign intelligence within its scope of oversight, and not only anti-terrorism.[40]

As for establishing in the UK something akin to the US's PCLOB, the Government declared an intention to legislate for a Privacy and Civil Liberties Board (PCLB), eschewing the word 'oversight' in its title. Many, including Anderson, looked askance at a PCLB; Anderson's role as IPR, the Independent Reviewer of Terrorism Legislation, it was envisaged, would be replaced by this new body, or at least to be assisted by such a body whose remit and purpose were not clear and appeared unnecessary. In the event, a PCLB was passed into law as the general and opaque Section 46 of the Counter-Terrorism and Security Act 2015, but requiring secondary legislation for its implementation and with no certainty that this would ever be implemented. Its very name — suggesting a privacy-and-civil-liberties function and remit — seems belied by the bare outline of these as given in the Act.[41]

It is a well-grounded observation that technological change outpaces the capacity of law (and lawmakers, judges and overseers)

38 The President's Review Group on Intelligence and Communications Technologies (2014), p. 15.

39 For historical details, see Hatch.

40 The President's Review Group on Intelligence and Communications Technologies (2014), pp. 195–99.

41 For critical comment on this, see Cols. 307–18 of the House of Lords, *Lords Hansard Text for 28 Jan 2015 (Pt 0003)* (London: HMSO, 2015), http://www.publications.parliament.uk/pa/ld201415/ldhansrd/text/150128-0003.htm

to catch up for the purpose of regulation in the interest of human rights — including privacy — and other values. This observation is no less relevant to intelligence oversight, in which the practices that are overseen rely heavily on technologically very complex and often arcane means of information gathering and analysis. It is therefore appropriate to mention the way in which recent reports have touched on the question of how technological knowledge can be brought to bear effectively in oversight arrangements. The Review Group Report considered the creation of an Office of Technology Assessment (OTA) within the CLPP Board to be useful 'to assess Intelligence Community technology initiatives and support privacy-enhancing technologies'.[42] 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'.[43]

Circumstances within the UK prevent any simple borrowing from the example of other countries' institutions, and technology assessment in the Federal Government has its own institutional and political backstory that shapes present recommendations. But the Review Group Report's suggestion of an OTA may have some greater traction in the UK, owing to an internationally shared need to keep abreast of the information and communication technology (ICT) instruments that are increasingly used in terrorism and crime. In the UK, the ability of overseers, let alone Government, Parliament, and the panoply of Commissioners operating in the security and intelligence field, to keep abreast of information and communication technology (ICT) developments and the worlds of the internet and 'data' remains a problem for the effectiveness of legislation and oversight, as was remarked upon in the three UK reports considered in this chapter.[44] Anderson referred to the views he received

42 Privacy impact assessment (PIA) has become a widespread technique for information systems and technologies, see David Wright and Paul De Hert, *Privacy Impact Assessment* (Dordrecht: Springer Netherlands, 2012); among the organisations that conduct PIA is the US's Department of Homeland Security, see Department of Homeland Security, *Privacy Impact Assessments* (24 August 2015), https://www.dhs.gov/privacy-impact-assessments

43 The President's Review Group on Intelligence and Communications Technologies (2014), p. 198.

44 E.g. *A Question of Trust*, Chapter 4; Royal United Services Institute for Defence and Security Studies (2015), Chapter 1.

that emphasised the importance of involving technical specialists in the oversight process, whether as part of the oversight machinery or playing supporting roles.[45] In proposing the creation of an Independent Surveillance and Intelligence Commission (ISIC), he thought ISIC 'should be willing to draw on expertise from the worlds of intelligence, computer science, technology, academia, law and the NGO sector'.[46]

The RUSI report recommended the creation of an Advisory Council for Digital Technology and Engineering as a statutory non-departmental public body. It would:

> keep under review the domestic and international situation with respect to the evolution of the Internet, digital technology and infrastructure, as well as:
> - Provide advice to relevant ministers, departments and agencies on technical measures.
> - Promote co-operation between the public and private sectors.
> - Manage complaints from CSPs [communications service providers] on notices and measures they consider unreasonable.
> - Advance public education.
> - Support research on technology and engineering.[47]

Moreover, this Advisory Council would be a resource for the ISC and for the new proposed National Intelligence and Surveillance Office that is recommended to replace the present array of three Commissioners in this field.[48] Whether any of these alternatives will gain support cannot be foretold. However, as with the recommendation of an OTA in the US, they speak to a glaring need in the operations of security and intelligence oversight and democratic control. Whatever the status of the agencies' own knowledge of new and emerging technologies, overseers need sufficient knowledge to understand the technological side of the work of those they oversee, and to bring to bear upon it their independent critical intelligence and their sense of the rights and values at stake. Such knowledge may help them to shape the questions they ask of agencies — and to interrogate the answers — whose vested interests may not always align with the interests, rights or needs of those whom they

45 *Ibid*., p. 236.
46 *Ibid*., p. 305.
47 Royal United Services Institute for Defence and Security Studies (2015), pp. 107–08.
48 *Ibid*., p. 108.

are tasked to protect. This problem is acknowledged universally, but there is no easy, and no prominent, agenda for a solution in the rapidly changing circumstances of threats and of the technological means both to carry them out and to frustrate prevention, detection and apprehension.

Conclusion

This chapter has dealt briefly with some conceptual and practical issues in the oversight of security and intelligence services, and in the wider field of human rights or civil liberties that are affected by these services and by their oversight as well. It has sought to highlight difficulties and ambiguities that stalk the attempt to improve the way a democratic society and political system attempts to 'civilise security', to borrow a term from the academic literature.[49] It is appropriate to end with a question that puts the point clearly:

> What kind of institutional matrix is likely to permit [the state] to be able to exercise sufficient vertical oversight and control over the plurality of agents and agencies who today promise to deliver security, whilst at the same time ensuring that the state anchor remains, in both its delivering and regulatory dimensions, subject to adequate democratic contestation and public and legal scrutiny?[50]

The areas touched on in this chapter resonate with two of the elements of an 'institutional matrix' — rights and resources — proposed by Loader and Walker,[51] but much further analysis is needed to explore how better thinking about privacy, security, independent oversight and its machinery, and technological understanding, might take their place in a matrix, without welding them into a rigid pattern that cannot be altered as new circumstances arise.

49 Loader and Walker (2007).
50 *Ibid*., p. 215.
51 *Ibid*., Chapter 8.

References

Anderson, David, *A Question of Trust: Report of the Investigatory Powers Review* (London: HMSO, 2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf

Bellaby, Ross, 'What's the Harm? The Ethics of Intelligence Collection', *Intelligence and National Security*, 27 (2012), 93–117, http://dx.doi.org/10.1080/02684527.2012.621600

Bennett, Colin and Raab, Charles, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge, MA: MIT Press, 2006).

Chandler, Jennifer, 'Privacy Versus National Security: Clarifying the Trade-Off', in *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, ed. by I. R. Kerr, V. M. Steeves and C. Lucock (Oxford: Oxford University Press, 2009), pp. 121–38.

Cohen, Julie E., *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale: Yale University Press, 2012).

Defty, Andrew, 'Educating Parliamentarians About Intelligence: The Role of the British Intelligence and Security Committee', *Parliamentary Affairs*, 61 (2008), 621–41, http://dx.doi.org/10.1093/pa/gsn024

Department of Homeland Security, 'Privacy Impact Assessments' (24 August 2015), https://www.dhs.gov/privacy-impact-assessments

Etzioni, Amitai, *Security First: For a Muscular, Moral Foreign Policy* (Yale: Yale University Press, 2008).

Finn, Rachel L., Wright, David, and Friedewald, Michael, 'Seven Types of Privacy', in *European Data Protection: Coming of Age*, ed. by Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet (Dordrecht: Springer Netherlands, 2013), pp. 3–32.

Foreign and Commonwealth Office and the Rt Hon Philip Hammond, 'Foreign Secretary Intelligence and Security Speech', Gov.uk, 15 March 2015, https://www.gov.uk/government/speeches/foreign-secretary-intelligence-and-security-speech

Fredman, S., 'The Positive Right to Security', in *Security and Human Rights*, ed. by B. J. Goold and Liora Lazarus (Oxford: Hart, 2007), pp. 307–24.

Gill, Peter, 'Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the "War on Terror"', *Intelligence and National Security*, 22 (2007), 14–37, http://dx.doi.org/10.1080/02684520701200756

—, 'The Intelligence and Security Committee and the Challenge of Security Networks', *Review of International Studies*, 35 (2009), 929–41, http://dx.doi.org/10.1017/S0260210509990362

—, 'Intelligence, Threat, Risk and the Challenge of Oversight', *Intelligence and National Security*, 27 (2012), 206–22, http://dx.doi.org/10.1080/02684527.2012.661643

Goold, Benjamin J., 'Surveillance and the Political Value of Privacy', *Amsterdam Law Forum*, 1 (2008), 3–6, http://heinonline.org/HOL/Page?handle=hein.journals/amslawf1&g_sent=1&collection=journals&id=389

Halchin, L. E. and Kaiser, F., *Congressional Oversight of Intelligence: Current Structure and Alternatives* (Washington, DC: Congressional Research Service, 2012).

Hatch, Garrett, *Report for Congress Privacy and Civil Liberties Oversight Board: New Independent Agency Status* (Washington DC, 2012).

House of Lords, *Lords Hansard Text for 28 Jan 2015 (Pt 0003)* (London: HMSO, 2015), http://www.publications.parliament.uk/pa/ld201415/ldhansrd/text/150128-0003.htm

House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State, 2nd Report of Session 2008–09, Hl Paper 18-I* (London: HMSO, 2009), http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm

Ilves, Toomas Hendrik, '"Rebooting Trust? Freedom *vs* Security in Cyberspace" Opening Address at Munich Security Conference Cyber', Office of the President, Republic of Estonia (Munich, 31 January 2014), https://vp2006-2016.president.ee/en/official-duties/speeches/9796-qrebooting-trust-freedom-vs-security-in-cyberspaceq

Independent Reviewer of Terrorism Legislation, *Investigatory Powers Review Written Submissions (H-V)* (London: Independent Reviewer of Terrorism Legislation, 2015), https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/Submissions-H-Z.pdf

Intelligence and Security Committee of Parliament, 'Privacy and Security Inquiry — Call for Evidence', 11 December 2013, https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20131211_ISC_Call_for_papers-Privacy.pdf

—, *Privacy and Security: A Modern and Transparent Legal Framework* (London: HMSO, 2015), https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt(web).pdf

Lazarus, L., 'Mapping the Right to Security', in *Security and Human Rights*, ed. by B. J. Goold and Liora Lazarus (Oxford: Hart, 2007), pp. 325–46.

Leigh, Ian, 'Rebalancing Rights and National Security: Reforming UK Intelligence Oversight a Decade after 9/11', *Intelligence and National Security*, 27 (2012), 722–38, http://dx.doi.org/10.1080/02684527.2012.708525

Lever, Annabelle, *Democracy, Privacy and Security* (Rochester: Social Science Research Network, 2015).

Loader, Ian and Walker, Neil, *Civilizing Security* (Cambridge: Cambridge University Press, 2007).

Lukes, Steven, *Power: A Radical View* (Basingstoke and New York: Palgrave Macmillan, 2004).

National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Authorized Edition) (New York: W. W. Norton & Company, 2011).

Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2009).

Phythian, Mark, 'Still a Matter of Trust: Post-9/11 British Intelligence and Political Culture', *International Journal of Intelligence and Counter Intelligence*, 18 (2005), 653–81, http://dx.doi.org/10.1080/08850600500177127

—, 'The British Experience with Intelligence Accountability', *Intelligence and National Security*, 22 (2007), 75–99, http://dx.doi.org/10.1080/02684520701200822

Raab, Charles, 'From Balancing to Steering: New Directions for Data Protection', in *Visions of Privacy: Policy Choices for the Digital Age*, ed. by C. Bennett and R. Grant (Toronto: University of Toronto Press, 1999), pp. 68–93.

—, 'The Meaning of "Accountability" in the Information Privacy Context', in *Managing Privacy through Accountability*, ed. by D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland and H. Postigo (London: Palgrave Macmillan, 2012), pp. 15–32.

—, 'Privacy, Social Values and the Public Interest', in *Politik Und Die Regulierung Von Information*, ed. by A. Busch and J. Hofmann (Baden-Baden: Nomos, 2012), pp. 129–51.

—, 'Privacy as a Security Value', in *Jon Bing: En Hyllest/A Tribute*, ed. by D. W. Schartum, L. Bygrave and A. G. B. Bekken (Oslo: Gyldendal, 2014), pp. 39–58.

Rascoff, Samuel J., 'Presidential Intelligence', *Harvard Law Review*, 129 (2016), 633–717, https://ssrn.com/abstract=2714769

Regan, Priscilla M., *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: University of North Carolina Press, 1995).

Royal United Services Institute for Defence and Security Studies, *A Democratic Licence to Operate: Report of the Independent Surveillance Review* (London: Royal United Services Institute for Defence and Security Studies, 2015).

Schattschneider, Elmer E., *The Semisovereign People: A Realist's View of Democracy in America* (New York: Holt, Rinehart and Winston, 1960).

Schoeman, Ferdinand David, ed., *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press, 1984).

—, *Privacy and Social Freedom* (Cambridge: Cambridge University Press, 1992).

—, and Solove, Daniel J., *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008).

Sookman, Barry, 'Internet Users' Privacy and Anonymity Protected by Supreme Court: *R v. Spencer*', 13 June 2014, http://www.barrysookman.com/2014/06/13/internet-users-privacy-and-anonymity-protected-by-supreme-court-r-v-spencer/

Steeves, V., 'Reclaiming the Social Value of Privacy', in *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, ed. by I. R. Kerr, V. M. Steeves and C. Lucock (New York: Oxford University Press, 2009).

The President's Review Group on Intelligence and Communications Technologies, *The NSA Report: Liberty and Security in a Changing World* (Princeton and Oxford: Princeton University Press, 2014).

US Congress, *Public Law 110–53, 110th Congress—Aug. 3, 2007: Implementing Recommendations of the 9/11 Commission Act of 2007* (Congress.gov, 2007), https://www.congress.gov/bill/110th-congress/house-bill/1

Waldron, Jeremy, 'Security and Liberty: The Image of Balance', *Journal of Political Philosophy*, 11 (2003), 191–210, http://dx.doi.org/10.1111/1467-9760.00174

Wright, David and De Hert, Paul, eds., *Privacy Impact Assessment* (Dordrecht: Springer Netherlands, 2012).

Wright, David and Raab, Charles, 'Privacy Principles, Risks and Harms', *International Review of Law, Computers & Technology*, 28 (2014), 277–98, http://dx.doi.org/10.1080/13600869.2014.913874

Zedner, Lucia, 'The Concept of Security: An Agenda for Comparative Analysis', *Legal Studies*, 23 (2003), 153–75, http://dx.doi.org/10.1111/j.1748-121X.2003.tb00209.x

—, 'Seeking Security by Eroding Human Rights: The Side-Stepping of Due Process', in *Security and Human Rights*, ed. by Benjamin J. Goold and Liora Lazarus (Oxford: Hart, 2007), pp. 257–77.

—, *Security: Key Ideas in Criminology Series* (London and New York: Routledge 2009).

This book need not end here…

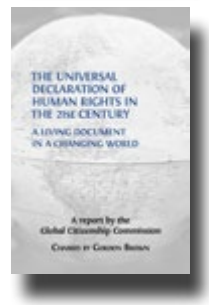
You may also be interested in:

The Infrastructure Finance Challenge
Edited by Ingo Walter

https://www.openbookpublishers.com/product/544

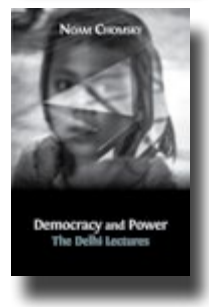
The Universal Declaration of Human Rights in the 21st Century
Edited by Gordon Brown

https://www.openbookpublishers.com/product/467



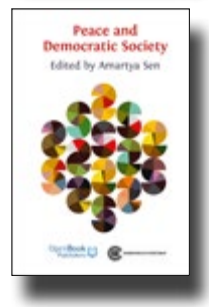
Democracy and Power
The Delhi Lectures
Noam Chomsky. Introduction by Jean Drèze

https://www.openbookpublishers.com/product/300



Peace and Democratic Society
Edited by Amartya Sen

http://www.openbookpublishers.com/product/78



Security in a Small Nation

Scotland, Democracy, Politics

Andrew W. Neal (ed.)

The 2014 Referendum on Scottish independence sparked debate on every dimension of modern statehood. Levels of public interest and engagement were unprecedented, as demonstrated by record-breaking voter turnout. Yet aside from Trident, the issue of security was relatively neglected in the campaigns, and there remains a lack of literature on the topic. In this volume Andrew Neal has collated a variety of interdisciplinary perspectives on security and constitutional change in Scotland and the UK, including writing from experts in foreign policy analysis, intelligence studies, parliamentary studies, and journalism.

Security in a Small Nation provides an illuminating analysis of the politics of security. Its authors reflect on a number of related issues including international comparisons, alliances, regional cooperation, terrorism, intelligence sharing, democratic oversight, and media coverage. It has a particular focus on what security means for small states and democratic politics.

The book draws on current debates about the extent of intelligence powers and their implications for accountability, privacy, and human rights. It examines the foreign and security policy of other small states through the prism of Scottish independence, providing unique insight into the bureaucratic and political processes associated with multi-level security governance. These contributions provide a detailed picture of the changing landscape of security, including the role of diverse and decentralised agencies, and new security interdependencies within and between states.

The analysis presented in this book will inform ongoing constitutional debates in the UK and the study of other secessionist movements around the world. *Security in a Small Nation* is essential reading for any follower of UK and Scottish politics, and those with an interest in security and nationhood on a global scale.

As with all Open Book publications, this entire book is available to read for free on the publisher's website. Printed and digital editions, together with supplementary digital material, can also be found here: www.openbookpublishers.com

Cover image: Scottish Parliament (2011)
Cover Design: Heidi Coburn

ebook
ebook and OA editions also available

OpenBook Publishers

Open Report Series