2-1-2011

One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty (Introduction)

Simon Chesterman
New York University School of Law, chesterman@nus.edu.sg

One Nation Under Surveillance

A New Social Contract to Defend Freedom Without Sacrificing Liberty

SIMON CHESTERMAN

OXFORD
UNIVERSITY PRESS

2011

Contents

Introduction: The End of Privacy

> There was of course no way of knowing whether you were being watched at any given moment. . . . It was even conceivable that they watched everybody all the time.
>
> George Orwell, *Nineteen Eighty-Four*[1]

Soon after his appointment as US Secretary of State in 1929, Henry Stimson was shown several Japanese communications that had been intercepted and deciphered by the State Department's small, highly classified Cipher Bureau, known informally as the Black Chamber. His immediate and violent reaction was that such subterfuge was 'highly unethical' and that the State Department could have nothing to do with it. The annual budget of $25,000 was effectively cut off, its six staff retrenched, and the Black Chamber was forced to close. Writing in his memoirs some years later, Stimson explained his firm belief that 'Gentlemen do not read each other's mail.'[2]

Eighty years later, the National Security Agency (NSA) is the successor to the Black Chamber. Its staff now number more than 30,000, with a classified budget estimated at well over ten billion dollars. Created soon after the Second World War, most Americans had never heard of it until the mid-1970s. (For decades its acronym was said to stand for 'No Such Agency'.) NSA activities were long the subject of hyperbolic speculation, but a few years after the end of the Cold War a comparatively sober report to the European Parliament noted that all e-mail, telephone, and fax communications on

[1] George Orwell, *Nineteen Eighty-Four* (London: Secker and Warburg, 1949), 9.

[2] Herny L Stimson and McGeorge Bundy, *On Active Service in Peace and War* (New York: Harper and Brothers, 1947), 188; William F Friedman, 'From the Archives: A Brief History of the Signal Intelligence Service (June 1942; declassified 1979)', *Cryptologia* 15(3) (1991) 263 at 266–8.

the continent were routinely intercepted.[3] Working with allies such as Britain and Australia, and with much of the world's Internet traffic passing through US territory, the United States now enjoys a level of information superiority unprecedented in the history of espionage.

Spying on foreigners has long been regarded as an unseemly but necessary enterprise. The laws of war, for example, allow for the use of spies—but if those spies are captured they are not entitled to prisoner-of-war status and may be executed. International law tolerates intelligence activities and even, in areas such as arms control, protects it. Spying on one's own citizens in a democracy, by contrast, has historically been subject to various forms of domestic legal and political restraint. For most of the twentieth century these regimes were kept distinct organizationally and legally, with foreign and domestic intelligence pursued by separate agencies governed by different rules. The US Central Intelligence Agency (CIA) and Britain's Secret Intelligence Service (MI6) operated abroad with few constraints; their domestic counterparts, the intelligence element of the Federal Bureau of Investigation (FBI) and Britain's Security Service (MI5) had more restrictions on their activities and cooperated to varying degrees with the regular police. Surveillance of agents of foreign powers was permissible; spying on citizens generally was not. There were, to be sure, violations of these principles—spectacularly culminating in Watergate and the resignation of President Nixon. Such scandals reinforced the view that foreign and domestic intelligence should and could be kept apart.

That position is no longer tenable. Three factors are driving the erosion of the distinction. First, and most obviously, many of the threats facing modern democracies do not respect national borders. It is important not to overstate the threat posed by terrorism: over the past four decades, the number of Americans killed by international terrorists was about the same as the number killed by lightning strikes or allergic reactions to peanuts.[4] Nevertheless, for the foreseeable future, the most significant

[3] Steve Wright, An Appraisal of the Technologies of Political Control (Brussels: European Parliament, STOA Interim Study, PE 166.499/INT.ST, 1998). See generally James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency* (Boston: Houghton Mifflin, 1982); James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York: Doubleday, 2008).

[4] Philip Bobbitt, *Terror and Consent: The Wars for the Twenty-First Century* (New York: Allen Lane, 2008), 7.

threat of violence on US or British soil will come from terrorists who do not have an obvious state sponsor that could be deterred or coerced: the targets of intelligence services will therefore be individuals rather than states.

The second factor is the revolution in technology and communications. Linked to developments in transportation and the enmeshing of diverse economies described by the loose term 'globalization', the increased use of electronic communications has been matched by the development of ever more sophisticated tools of surveillance. It has also blurred the distinction between what is foreign and what is domestic. The idea that the NSA, for example, can intercept e-mails sent by foreigners but not by US citizens poses—apart from anything else—technical challenges: when a message is routed through strings of Internet service providers, it is not always clear what is 'foreign' and what is 'local'. In any case, there are frequent reports citing analysts within the NSA to the effect that restrictions are not rigorously enforced.[5]

Thirdly, changes in culture are progressively reducing the sphere of activity that citizens can reasonably expect to be kept from government eyes. This is most obvious in the amount of information voluntarily disclosed through social-networking Web sites and the use of loyalty cards, as well as the increased toleration of closed-circuit television (CCTV) in public spaces. It is also implicit in the use of e-mail, credit cards, and other everyday transactions where significant amounts of personal information are passed on to corporations, the government, or both. The trend is likely to grow as personal data are increasingly stored online or 'in the cloud', facilitating access to information by users from a variety of devices, but also placing that information in the hands of an ever-widening circle of actors.[6]

The main casualty of this transformed environment will be privacy. Though privacy is invoked with respect to many aspects of life, the term is used here primarily in the sense of information. Assertions of a *right* to privacy can be understood as the claim of an individual to determine for

[5] See, eg, James Risen and Eric Lichtblau, 'E-mail Surveillance Renews Concerns in Congress', *New York Times*, 16 June 2009.

[6] See Jonathan Zittrain, *The Future of the Internet—and How to Stop It* (New Haven, CT: Yale University Press, 2008).

him- or herself when, how, and to what extent information about him or her is communicated to others.[7] Though the desire to keep certain information about oneself private has ancient origins, the modern 'right' is commonly traced to late nineteenth century developments in the United States, where it was the legal response to changed threats, technology, and culture: the rise of sensationalistic journalism, the invention of the hand-held camera, and changing views on the proper role of mass media.[8]

Similar factors were at work through the twentieth century as different balances were struck between the desire of the state to understand and pre-empt threats and the desire of individuals 'to be let alone'.[9] The latter half of the century saw an explosion in literature dealing with the question, with prescient warnings about computerization increasing the amount of information available to governments and other actors, as well as the ease of accessing it.[10] Revelations of abuse or constitutional upheavals periodically slowed it down, but the inexorable trend has been towards greater collection and aggregation of data. That trend only accelerated with the rise of the Internet.

In recent years, the battleground of privacy has been dominated by fights over warrantless electronic surveillance in the United States and CCTV in Britain; the coming years will see further debates over DNA databases, data mining, and biometric identification. There will be protests and lawsuits, editorials and elections resisting these attacks on privacy.

Those battles are worthy. But the war will be lost. Efforts to prevent governments from collecting such information are doomed to failure because modern threats increasingly require that governments collect it, governments are increasingly able to collect it, and citizens increasingly accept that they *will* collect it.

[7] Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1967), 7. Cf James B Rule, *Privacy in Peril* (Oxford: Oxford University Press, 2007), 3; Jon L Mills, *Privacy: The Lost Right* (Oxford: Oxford University Press, 2008), 13–27.

[8] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy', *Harvard Law Review* 4 (1890) 193; Westin, *Privacy and Freedom*, 8–22; Richard F Hixson, *Privacy in a Public Society* (Oxford: Oxford University Press, 1987), 3–25. Some European jurisdictions had embraced similar rights earlier than this. See, eg, *L'affaire Rachel* (Tribunal civil de la Seine, 16 June 1858). See further Chapter eight, section 4.

[9] This formulation derives from Thomas M Cooley, *A Treatise on the Law of Torts, or the Wrongs Which Arise Independent of Contract*, 2nd edn (Chicago: Callaghan & Co, 1888), 29.

[10] See, eg, Westin, *Privacy and Freedom*, 158.

There are, of course, limits to what citizens will tolerate. In 2002, for example, the Pentagon developed plans to fund research projects aimed at using information technology to identify and counter threats from terrorist actors. The plans were largely to draw on information already in the hands of government, but some bad choices doomed the project: labelling the goal as 'Total Information Awareness', adopting a logo with the all-seeing Eye of Providence from the pyramid on the Great Seal of the United States, and putting in charge an official who had been indicted for his role in the 1980s Iran–Contra affair.[11]

Nevertheless, the clear progression is towards ever greater government collection of information on the citizenry, and broad—though hardly universal—acceptance of that reality. The argument here is not that this is good or bad: it is, in many ways, an inevitable consequence of a modern and globalized life. Rather, the point of this book is to shift the focus away from questions of whether and how governments should *collect* information and onto more problematic and relevant questions concerning its *use*.

1. UNDERSTANDING INTELLIGENCE

In the shelf-straining literature on intelligence, three broad questions have dominated for over half a century. The first, given the secretive nature of much of the subject, is simply 'what happened?' Such books tend to cluster around the self-serving memoirs of former spies on the one hand, and the breathless accounts of outsiders on the other.[12] The second question concerns how to make sure that intelligence services have sufficient powers to do their job effectively, without acquiring so much power that they undermine or corrupt democratic government. These volumes lean

[11] Bobbitt, *Terror and Consent*, 261–3. One of the first articles raising the alarm against the programme was William Safire, 'You Are a Suspect', *New York Times*, 14 November 2002.

[12] Prominent examples include Bamford, *Puzzle Palace*; Peter Wright, *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer* (New York: Viking, 1987); Stephen Dorril, *MI6: Inside the Covert World of Her Majesty's Secret Intelligence Service* (New York: Free Press, 2000); Robert Baer, *See No Evil: The True Story of a Ground Soldier in the CIA's War on Terrorism* (New York: Three Rivers, 2002); Bamford, *Shadow Factory*.

towards either paternalistic expositions of the national security threats that civil libertarians cannot or will not understand, or the recitation of scandals and abuses of power that national security enthusiasts conveniently overlook.[13] Thirdly, there is a growing body of what one might call 'reform literature' that identifies systemic problems of analysis and coordination between agencies in the hope of improving the output of intelligence services without necessarily increasing the input. Here the dominant themes tend to be the need to liberate agents and analysts from bureaucracy and encourage individual excellence, or else to strengthen that bureaucracy in order to ensure that coordinated and coherent advice reaches policymakers.[14]

The result has been more heat than light, with surprisingly little serious academic treatment of the subject of intelligence.[15] What is missing in this literature is a clear-eyed account of how one can and should balance oversight and operational freedom—legitimacy and effectiveness—in the activities of intelligence services. This book addresses that tension directly and seeks to map out a new way of understanding intelligence in its modern context. Similar efforts have been undertaken with respect to particular questions—the US approach to torture, for example, or preventive detention—but the present work aims to cover a wider range of subjects (including electronic surveillance and information sharing between governments) across a spectrum of cases (notably comparing

[13] See, eg, Hans Born, Loch K Johnson, and Ian Leigh (eds), *Who's Watching the Spies: Establishing Intelligence Service Accountability* (Washington, DC: Potomac Books, 2005); Hans Born and Marina Caparini (eds), *Democratic Control of Intelligence Services: Containing Rogue Elephants* (Aldershot: Ashgate, 2007); Bobbitt, *Terror and Consent*; John Yoo, *Crisis and Command: A History of Executive Power from George Washington to George W Bush* (New York: Kaplan, 2010).

[14] See, eg, Richard A Posner, *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11* (Stanford, CA: Hoover, 2005); Richard K Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (New York: Columbia University Press, 2007); Robert M Clark, *Intelligence Analysis: A Target-Centric Approach*, 2nd edn (Washington, DC: CQ Press, 2007); Thomas E Copeland, *Fool Me Twice: Intelligence Failure and Mass Casualty Terrorism* (Leiden: Koninklijke Brill NV, 2007); Richard L Russell, *Sharpening Strategic Intelligence: Why the CIA Gets It Wrong and What Needs to Be Done to Get It Right* (Cambridge: Cambridge University Press, 2007); Amy B Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton: Princeton University Press, 2007); Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY: Cornell University Press, 2010).

[15] Amy B Zegart, 'Cloaks, Daggers, and Ivory Towers: Why Academics Don't Study US Intelligence', in Loch K Johnson (ed), *Strategic Intelligence* (Westport, CT: Praeger, 2007), 21.

the United States, Britain, and intelligence sharing within the United Nations).

'Intelligence' is understood here in two senses. In the abstract, it will be used to refer to information obtained covertly—that is, without the consent of the person or entity that controls the information. This is sometimes referred to as 'secret intelligence'. Within this heading, two subcategories of intelligence that have remained essentially unchanged since the Second World War are intelligence obtained wittingly or unwittingly from individuals, known as human intelligence or HUMINT, and signals intelligence or SIGINT, which comprises communications intercepts and other electronic intelligence. A newer subcategory is photographic or imagery intelligence (IMINT), now dominated by satellite reconnaissance. Many more -INTs appear in the literature, but these three will be the focus here.[16]

The abstract definition of intelligence is complemented by a broader understanding of the term as the analytical product of intelligence services, best understood as a risk assessment intended to guide action. These two definitions highlight an important distinction that must be made between the collection and the analysis of intelligence. Though collection may be covert, analysis should generally draw upon a far wider range of sources, most of which—frequently the vast majority—will be publicly available or 'open'. These discrete functions are reflected in the structure of most Western intelligence services: more by accident than design, the principle has evolved that those who collect and process raw intelligence should not also have final responsibility for evaluating it. The top-level product of such analysis is known in Britain as an assessment; in the United States the term estimate is used. This is distinct from how such analysis should inform policy—a far broader topic.[17]

These two uses of intelligence correspond roughly to a distinction sometimes made between 'secrets' and 'mysteries'. A secret is a knowable fact that can be stolen by a spy or intercepted by a technical sensor, such as

[16] See Michael Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press, 1996), 61–81. Wider definitions of intelligence are sometimes used, such as 'information designed for action', but this would appear to encompass any data informing policy at any level of decision-making. See generally Michael Warner, 'Wanted: A Definition of Intelligence', *Studies in Intelligence (Unclassified Edition)* 46(3) (2002) 15.

[17] Herman, *Intelligence Power*, 111–12.

the number of nuclear weapons possessed by a given country. A mystery is a puzzle to which no one can be sure of the answer, such as the likely response of a political leader to future events: no one can steal that answer; the leader may not know him- or herself.[18]

Intelligence services may have other functions such as covert action and counter-intelligence, but the focus here is on the acquisition of secrets and the resolution of mysteries. A key finding is that the increasing transparency of many aspects of modern life is reducing the number of secrets it is possible to keep from anyone.

2. OUTLINE OF THE BOOK

The book is organized into three parts. Part I addresses the modern political and legal context within which intelligence services operate, with the first Chapter reviewing the changing role of intelligence during and after the Cold War. Understanding the intentions and capacities of other actors has always been an important part of statecraft. Recent technological advances have increased the risks of ignorance, with ever more powerful weapons falling into ever more unpredictable hands. At the same time, other advances have lowered the price of knowledge: vastly more information is freely available and can be accessed by far more people than at any point in history. 'Secret intelligence', in the sense of information being obtained covertly, is thus both more and less important than it was during the Cold War.

The following two chapters address basic questions that run through the volume. *Should* intelligence activities by the state be constrained when those activities are intended to protect the life of the nation? And, regardless of how one answers that question, *can* intelligence activities be constrained in a meaningful way when those activities will necessarily be undertaken secretly?

Chapter two examines the unresolved debates over how democracies should respond to crises such as the 'ticking time-bomb' scenario, in which a terrorist knows the location of a bomb but will not talk. This is an

[18] Joseph S Nye, 'Peering into the Future', *Foreign Affairs* 73(4) (1994) 82 at 86–8.

extreme example of an emergency that may cause a state to bend or break its own laws. As Bruce Ackerman has wryly noted, only one major thinker of the twentieth century treated emergencies as a central theme of his work: 'and he, alas, turned out to be a Nazi'.[19] Debates over the limits of legality precede the writings of Carl Schmitt, however, and the Third Reich now offers a salutary warning of the dangers of excessive state power. Indeed, one of the most interesting aspects of twentieth century intelligence is that even as the powers of agencies tended to expand, so did the view that they should be grounded in law. This turn to law was severely challenged following the September 11 attacks on the United States.

Even if one concludes that intelligence services should be subject to the rule of law, it is generally accepted that some degree of secrecy is appropriate for their activities. The sociologist Edward Shils, writing soon after the McCarthy hearings had shaken the United States, argued that liberal democracy rested on protecting privacy for individuals and rejecting it for government.[20] The following half-century has seen the opposite happen: in addition to the erosion of privacy for individuals, governments have become ever more secretive. This is true with respect to the classification of information that governments now deem 'secret', but also with respect to efforts at oversight by other branches of government. Norman Mineta, who served on the House Intelligence Committee under Ronald Reagan, famously commented that legislative overseers were like mushrooms: the intelligence community kept them in the dark and fed them a lot of manure.[21] Chapter three discusses the limits of appropriate secrecy and the challenges it poses for effective accountability.

Part II turns to three cases that illustrate evolution in the practice of intelligence. The intention is not to provide an exhaustive account of intelligence practices in each jurisdiction, but rather to use them to examine how threats, technology, and culture have shaped that practice. Chapter four describes the United States and the upheavals caused by the response to September 11. Demands for effective responses by government to the threat of terrorism exerted understandable pressure towards a freer hand

[19] Bruce Ackerman, *Before the Next Attack: Preserving Civil Liberties in an Age of Terrorism* (New Haven, CT: Yale University Press, 2006), 56.

[20] Edward A Shils, *The Torment of Secrecy: The Background and Consequences of American Security Policies* (London: Heinemann, 1956), 21–5.

[21] David M Alpern, 'America's Secret Warriors', *Newsweek*, 10 October 1983, 38.

for intelligence services, with legal and political consequences that are still being revealed. One of the most troubling aspects of the contemporary US intelligence community is the extent to which these archetypically 'public' functions are now being carried out by private actors.

Chapter five examines the political and legal status of Britain's intelligence services, which were only formally established by law beginning in 1989. Until that time, the legal fiction was that intelligence officers were merely 'ordinary citizens'. The passage of legislation was largely a response to challenges that stemmed from Britain's accession to the European Convention on Human Rights. Britain therefore provides a useful case study of the turn to law, but also of the danger of formalizing the activities of intelligence services if mandates are not drawn carefully, and of the limited effect legislation may have on entrenched practices. The risks are particularly evident in the belated efforts to apply privacy rights to video surveillance after some four million CCTV cameras (about one for every 14 citizens) had been installed across the country.

Chapter six turns to the manner in which the response to transnational threats has led to a reassessment of how intelligence can be shared through international organizations. During the Cold War, intelligence was a 'dirty word' within the United Nations, but international cooperation on counterterrorism and other issues now depends on reliable and timely intelligence that is normally collected by states. The topic rose in prominence following the presentation of intelligence by the United States when attempting to justify the 2003 Iraq war, but is also relevant to targeted financial sanctions and international criminal prosecutions. The use of intelligence at the multilateral level is essential to address threats that do not respect borders, but reluctance to share sensitive information creates practical barriers that discourage sharing and poses legal problems when sharing does take place.

The three cases are interesting in themselves but also suggest broad themes for effective and legitimate intelligence: the essentially public nature of the power being exercised, the need to ground that power in the rule of law, and the importance of addressing not merely the collection of intelligence but its use by the state and all those with whom the intelligence is shared. The third and final part of the book draws on these themes to map out appropriate structures of accountability, the functions that can and should be subjected to those structures, and a framework to

understand the changed role of intelligence and respond to the challenges that it poses.

Chapter seven examines the most appropriate structures for ensuring the accountability of intelligence services. An important distinction must be made between control, oversight, and review, and the different roles that may be played by the executive, the legislature, and the judiciary, as well as civil society actors such as the media. Few accountability structures are established in a vacuum: indeed, a key determinant of the structures adopted in a given jurisdiction is the context in which reforms are undertaken. Change most commonly takes place after a scandal, with predictable consequences if that scandal was failure to prevent a terrorist attack, or overzealous efforts to prevent one.

Chapter eight considers whether the focus of accountability should be on the collection of intelligence or its use. Here it is important to distinguish the functions of law enforcement agencies from those of intelligence services, and to consider how the relationship between such governmental agencies should be managed. When secret intelligence would be useful in a criminal proceeding, what safeguards, if any, should be put in place to protect the rights of the accused? What safeguards should protect the sources and methods of the intelligence service? Increasingly, where such information is collected, it is unrealistic to assume that law enforcement agencies will not have access to it, regardless of any safeguards. Again, the better question appears to focus on the use of that information, with new safeguards required in a post-privacy world.

The final Chapter returns to the theme of whether and how intelligence activities can be regulated effectively, linking this to larger questions of the diminishing sphere of truly private activity and the growing coercive powers of the state. Historically, that relationship was thought of as a public/private dichotomy, marking a distinction between the political and the personal: under liberal theory the former was subject to legal regulation; the latter was not. The transformations of threats, technology, and culture described in this book show that the relationship between public and private no longer makes sense as a dichotomy and is instead best thought of as a dynamic. With the emergence of the modern state, philosophers such as Hobbes, Locke, Kant, and Rousseau posited a social contract that explained how the legitimacy of political authority derived from the consent of the governed: in essence, people give a centralized political

entity coercive powers in order to make organized society possible. What we are witnessing now is the emergence of a new social contract, in which individuals give the state (and, frequently, many other actors) power over information in exchange for security and the conveniences of living in the modern world.

3. FREEDOM AND LIBERTY

The surveillance state described in George Orwell's dystopian novel *Nineteen Eighty-Four* was perpetuated through coercion and deception. Orwell explicitly set his novel in Britain in order to emphasize that it was not an attack on communism and fascism alone, but a warning that 'totalitarianism, *if not fought against*, could triumph anywhere.'[22] It is revealing that 'Big Brother' was, in the late twentieth century, a warning cry used by civil libertarians to deplore attacks on privacy reminiscent of Orwell's surveillance state.[23] By the first decade of the twenty-first century, however, the term was most commonly linked to a reality television programme of the same name in which housemates are continually watched by television cameras.[24] 'The innocent have nothing to fear' was once the patronizing mantra of an authoritarian state. Increasingly, a new media savvy generation appears to embrace the view that 'the fearless have nothing to hide'. The change is not confined to young people or those ignorant of security protocols. In July 2009, it was revealed that the wife of the incoming head of MI6 had posted compromising information on a Facebook account, including the location of their London flat and the whereabouts of their three adult children.[25]

[22] George Orwell, Letter to Francis A. Henson, dated 16 June 1949, reprinted in Ralph Thompson, 'In and Out of Books', *New York Times*, 31 July 1949.

[23] See, eg, Shannon E Martin, *Bits, Bytes, and Big Brother: Federal Information Control in the Technological Age* (Westport, CT: Praeger, 1995); Simon Davies, *Big Brother: Britain's Web of Surveillance and the New Technological Order* (London: Pan Books, 1996).

[24] See, eg, Toni Johnson-Woods, *Big Bother: Why Did That Reality TV Show Become Such a Phenomenon?* (Brisbane: University of Queensland Press, 2002); Jonathan Bignell, *Big Brother: Reality TV in the Twenty-First Century* (New York: Palgrave Macmillan, 2005).

[25] Jason Lewis, 'MI6 Chief Blows His Cover as Wife's Facebook Account Reveals Family Holidays, Showbiz Friends and Links to David Irving', *Mail on Sunday* (London), 5 July 2009.

Arguments over the appropriate balance between liberty and security have a long pedigree in political theory.[26] During debates on the Patriot Act, for example, a US senator invoked the words of one of the founding fathers: 'As Ben Franklin once noted, "if we surrender our liberty in the name of security, we shall have neither."'[27] In fact Franklin's words were more nuanced: 'Those who would give up *essential* Liberty, to purchase a little *temporary* Safety, deserve neither Liberty nor Safety.'[28] This volume will not be the last word on how that balance should be struck. But it is hoped that by reframing the relationship between privacy and security in the language of a social contract, mediated by a citizenry who are active participants rather than passive targets, the book offers a framework to defend freedom without sacrificing liberty.

[26] See Chapter two, section 1.2.

[27] Patrick Leahy, 'The Uniting and Strengthening America Act of 2001', *Congressional Record (Senate)* 147(134) (2001) S10365 at S10366.

[28] Benjamin Franklin, 'Pennsylvania Assembly: Reply to the Governor, November 11, 1755', in Leonard W Labaree (ed), *The Papers of Benjamin Franklin* (New Haven, CT: Yale University Press, 1963) vol 6, 242 (emphasis added). See also Michael J Woods, 'Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215', *Journal of National Security Law & Policy* 1(1) (2005) 37 at 71; Bobbitt, *Terror and Consent*, 286.