“Delayed Disclosure”:

National Security, Whistle-blowers and the Nature of Secrecy

Richard J. Aldrich & Christopher R. Moran

Abstract

The significance of Edward Snowden’s revelations has been viewed primarily through the prism of threats to citizen privacy. We argue instead that the most dramatic change has been a decline of government secrecy, especially around national security. While the ethical aspects of state secrets and “whistle-blowing” have received recent attention, few have attempted to explain the dynamics of this growing climate of exposure. Our argument is largely technological and we ground our analysis in the changing nature of intelligence work, which is increasingly merging with big data. But we also identify a related cultural change: many intelligence contractors are at best agnostic about the national security state. Meanwhile, the Internet itself provides the perfect medium for the anonymous degradation of secrets. Because the main driver is technology, we suggest this trend is likely to accelerate, presenting national security chiefs with one of their biggest future challenges.

Introduction

Open societies are increasingly defended by secret means. Since the 9/11 terrorist attacks, spending on intelligence, security, counter-terrorism and cyber security has doubled and redoubled again, creating a vast secret empire. The English-speaking world spends over $100 billion a year on intelligence alone. In the United States, over five million people enjoy security clearances. The defence of democracy by furtive intelligence and security services that resist democratic control has long presented us

with a profound paradox (Born and Leigh, 2005: 16). The idea of sustaining a multinational ring of secrecy that is populated by millions of people has arguably transformed something that is puzzling into something that is increasingly improbable.

Advanced liberal democracies are committed to keeping their secrets. In the United States, an estimated $11 billion is spent every year on security classification, double the amount expended at the turn of the century (Shane, 2012). This figure does not include the statistics for the Central Intelligence Agency (CIA), the National Security Agency (NSA), the Defense Intelligence Agency (DIA), or the Office of the Director of National Intelligence (ODNI), whose budgets remain classified. In Australia, the government's program of security vetting costs the taxpayer an annual $350 million, with clearances required for even the most innocuous of public service jobs far removed from the national security realm, including librarians, museum staff, and veterinarians (Thompson, 2015). Meanwhile, governments are now more energetic than ever in using the courts to punish "whistle-blowers" as well as the journalists who work with them.

The Obama administration arrived at the White House in Washington promising to run the most transparent administration in history. Despite some early gestures towards transparency – for example, an Executive Order in December 2009 banning indefinite classification and advising officials not to follow the age-old mantra of "when in doubt, classify" – in reality it pursued the path of silence and censorship whenever it was confronted by challenge. To the dismay of human rights activists Obama used the 1917 Espionage Act to prosecute more whistle-blowers than all his predecessors combined. Many of these issues were not related to national security but instead related to waste, corruption and fraud within government. His successor in the White House, Donald J. Trump, could well break this record. Less than a year into office, he has

already made bold promises on Twitter to root out "low-life leakers" in the government (van Buren, 2012; Moran & Aldrich, 2017).

However, while the appetite for secrecy remains strong, the ability to achieve it has never looked weaker, largely due to new electronic platforms. Since 2010 and the publication by WikiLeaks of 250,000 diplomatic cables from US embassies and consulates around the world, plus some half a million records from the conflicts in Iraq and Afghanistan, "document dumps" of sensitive information have become commonplace and part of a new media landscape. Known as "Cablegate", the leaking of US embassy cables by WikiLeaks was said by the State Department to have put the lives of US informants at risk, whilst foreign leaders embarrassed by the leaked material sent angry private letters to Washington demanding apologies. On 29 October 2013 at a Goldman Sachs summit in Arizona, former US Secretary of State Hillary Clinton told the audience of bankers that she was forced to go on a 'global apology tour' after Cablegate, adding, only half in jest, that she witnessed statesmen in tears. More recently, Clinton herself was caught in the tidal wave of disclosure, with some 30,000 of her private emails whilst Secretary of State being published by WikiLeaks at a critical moment in the 2016 presidential election campaign. She and her top aides believe that this may have cost her the White House (Friedman 2015).

Most impacted by the tsunami of electronic transparency have been intelligence and security agencies like the American NSA and Britain's Government Communications Headquarters (GCHQ), together with the various tech giants like Google, Facebook, and Verizon that have formed witting or unwitting partnerships with secret bodies. Famously, in June 2013, Edward Snowden leaked to the *Washington Post* and the *Guardian* an estimated 200,000 documents detailing highly classified US/UK surveillance programs, sparking an international furore. More recently, the CIA has

been embarrassed by the loss of the hacking tools it uses to compromise smart phones and televisions, turning them into improvised surveillance devices. Unsurprisingly, these disclosures have placed officials in London and Washington on notice, fearing what will be revealed next.

Precisely because these secret agencies have chosen to weaponize the Internet they have provoked protest from external constituencies. Many software developers and IT specialists still identify with figures like web guru and political activist John Perry Barlow, who articulated a utopian high-tech libertarianism and penned a declaration of independence for the Internet. Privacy campaigners and hacktivists also envisaged the Internet as part of a utopian realm in which the new information and communication technologies would change the ways in which citizens communicate, collaborate and indeed pursue political activism (Kelty, 2005). These groups, which might be conceptualized as online social movements, are vigorously committed to the demise of government secrecy, not least because they see the secret state as a direct threat to their own space, undermining everything that makes the Internet creative and free, while generating paranoia. David Lyon has suggested that the Snowden revelations are of the biggest importance for those concerned about the future of the Internet (Lyon, 2015b). Others have insisted that Snowden alerts us to a military-information-complex in which a few powerful companies are in league with the surveillance state (Fuchs, 2015).

Because the Snowden phenomenon has been largely analysed thought the prism of citizen privacy there is surprising dearth of research on the decline of state secrecy. Despite some recent normative and ethical contributions (Leigh & Harding, 2011; Lester, 2015; Sagar, 2013: Schoenfeld, 2011) we know little about what is actually going on in this realm. Instead, social scientists have tended to focus on new

surveillance technologies and their potential dystopian consequences for civil liberties (Gates, 2011; Goold, 2004; Rule, 2007; Vincent, 2016; Wicker, 2013). A significant body of literature has emerged on Snowden, but the analysis is largely through the lens of growing ethical concerns about the ability of governments to monitor every aspect of our digital lives (Bauman et al 2014, Edgar, 2017; Greenwald, 2014; Harding, 2014; Johnson, 2014; Lyon, 2015a). Partly as a result of recent interest in language, identity and the social construction of security, the subject of privacy, which concerns people and public discourse, is in scholarly vogue, especially when compared to the conventional and cloistered world of bureaucrats. The only exception is perhaps economists who have begun to model the transaction costs of secrecy within both liberal and planned economies (Harrison, 2013). However, we would we argue that while the changing nature of privacy over the last decade is undoubtedly important, it is only part of the picture. As much as there is a "crisis of privacy", there is also a "crisis of secrecy". From the perspective of officials, the most worrying issue is not government looking at us – but us looking at government. Secrecy, as Arthur Schlesinger Jr. (1987) wrote, is a source of state power. It enables governments to plan, predict and even forecast, away from glare of their enemies and free from the hubbub of the political marketplace. Less benignly, it is also a way to cover up 'embarrassments, blunders, follies and crimes of the ruling regime' (Schlesinger, 1987). Understandably, therefore, officials look at recent developments with alarm.

This article seeks to explore and understand the drivers behind this current crisis of secrecy. In an important intervention, published in 1998, Ann Florini suggested that governments and corporations were being pulled into the open by the triple processes of democratization, globalization and information technology, writing: 'With the spread of democratic norms, it seems right that powerful entities such as states and

corporations should be held accountable for their behaviour. Now, as the world shrinks, a lot of people want to have a say in what used to be other people's business'. Florini connected this process closely with globalization, insisting that ever-tightening connections created by trade resulted in strong pressures for better ways to govern the growing number of transnational interactions (1998). In areas as diverse as environmental politics and the regulation of financial markets there has been a growing assumption that transparency is one of the keys to effective governance (Gupta, 2008).

More recently, Florini has suggested that national security has become a realm of increasing exception, one where 'transparency gives way to secrecy'. In the post-9/11 era she warned that the 'growing US penchant [for secret government] … threatens to undermine a global trend toward greater transparency everywhere' (Florini, 2004). In this context, she pointed to the Patriot Act and Homeland Security Act, passed in 2001 and 2002 respectively, which introduced numerous provisions blocking citizen access to information. Yet despite considerable efforts to shore up state secrecy and the vast expenditure of resource, it is clear that this initiative is failing – and here we ask why? We argue that the Snowden leaks were symptomatic of wider and more important trends, including systematic changes in the nature of computing, together with the cultural attitudes of security contractors and the IT community. These trends increasingly overlap with an expanded intelligence community, the ability to share large volumes of data with allies, and the very nature of intelligence itself wherein the sources are themselves becoming increasingly unsecret. Indeed, we suggest that the very idea of 'secret intelligence' is beginning to look like a twentieth century concept and might well need to be revisited.

Tacitly, leading western intelligence agencies have already begun to accept that secrets now decline more rapidly, often in unpredictable ways. In the 1990s,

intelligence agencies in the UK embraced avowal and legal identities after years of dogged resistance and then discovered, to their surprise, that public acknowledgment of their existence did not cause them to melt into air (Phythian, 2007). Now, we are seeing an unexpected desire by the secret agencies to undertake public education, accepting that the failure to explain has a higher cost in an era when hacktivists potentially capture the moral high ground. Some of these changes are cultural but the main drivers are "big data" and new information and communication technology, the pace of which continues to accelerate remarkably. The outcome, to quote retired counterterrorism officer Mark Fallon, is a world in which 'there are no secrets, only delayed disclosures' (Watts, 2012).

Theories of Secrecy

The pioneering work on conceptions of secrecy has largely been undertaken by sociologists who have seen it as dependent on changing social relations. Writing in 1908, Georg Simmel associated both surveillance and secrecy with the advance of modernity. He argued that in pre-modern society, a person's immediate circle encompassed most of their existence, and so secrecy of any kind was difficult to achieve. By contrast, modern society saw a larger number of differentiated spaces and specialised roles, together with an increasing separation of the public and private spheres, and with this complexity came the increased possibility of secrecy (Marx and Muschert 2009; Curtin 2014).

The strongest secrecy has been associated with a government monopoly of special types of information, often designed to accelerate the tactical efficiency of defence and foreign policy. Governments have jealously guarded the power to

intentionally conceal information and the legal right to decide about disclosure. This sort of secrecy has had a dyadic quality; the wider population are often not aware that these government secrets even exist, something that has been termed 'double secrecy' or 'deep secrecy' (Pozen, 2010). Meanwhile, the most effective secrets are those obtained without the opponent knowing that this has happened, as in the case of wartime codebreaking at Bletchley Park, the so-called "Ultra Secret". Secret intelligence has thus been defined as other people's secrets stolen secretly (Robertson, 1987: 46).

Secrecy is often about government because it depends upon elaborate compartmentalization and classification. Accordingly, official secrecy has been constructed through a ritualistic system of distinguishing insiders from outsiders, with the highest clearances perceived as a form of status indicator (Schoenfeld 2010). Costas and Gray have remarked on the 'architectural' quality of secrecy, denoting those on the centre and those consigned to the periphery (2016). Some have suggested that national security officials have come to view high levels of secrecy as intrinsic to their work, irrespective of whether there was a genuine need for it. Moynihan and Vincent have both argued that, in its most elaborate form, this spawned a 'culture of secrecy' in which 'secrecy for secrecy's sake' became a defining characteristic of government (Moynihan 1999; Vincent 1998).

Max Weber, writing towards the end of the First World War, was the first to identify this culture of secrecy. He argued that this attitude stretched far beyond those areas where circumstances might justify the demand for secrecy, or might even be convenient: 'The concept of the "official secret" is the specific invention of bureaucracy, and nothing is so fanatically defended by the bureaucracy as this attitude, which cannot really be justified beyond these specifically qualified areas.' In other

words, bureaucratic secrecy had moved beyond merely covering up mistakes and abuses; it had become an end in itself. Weber argued that the security state's fascination with secrecy had undermined the functioning of government and was at the centre of a failed war effort (Weber 1918: 730-31).

Building on earlier conceptualisations, Steven Aftergood has identified three types of government secrecy. First, genuine national security secrecy that relates to the sort of information which, if disclosed, would damage public interests. Second, 'political secrecy', which involves the deliberate employment of classification to hide abuses or government failure. And third, a pathological culture of secrecy that views everything as secret unless it is deemed otherwise. Importantly, Aftergood argues that secrecy and the production of knowledge are fundamentally in conflict, since scientific enterprise and academic research asserts the essential importance of the open exchange of information, which is the natural obverse of secrecy (Aftergood 2008: 399, 401-3). Complementing this analysis, albeit from a different disciplinary standpoint, Zygmunt Bauman et al have written about the changing nature of dichotomies between national/international, public/private, state/society, foreign/domestic, friend/foe, and the transmogrification of traditional clear-cut Weberian coordinates into a new interconnected topology of security, encapsulated by the metaphor of the 'Möbius strip' – a one-sided surface where the inside and the outside become blurred (Bauman et al: 2014). It is precisely this collision of the old world of state secrecy and intelligence with the new world of innovation, information and interconnectivity, together with its impact on changing social relations, that we wish to explore here.

Big Data and Knowledge Intensive Security

The early twenty-first century is already being defined by big data computing across multiple domains together with remarkable interoperability and personal connectivity. The speed and scale of change is remarkable. IBM has estimated that 90% of the world's data has been created in the last two years, with human beings generating a stunning 2.5 quintillion bytes of data every day. In 2012, the world sent over eight trillion text messages. Many farm animals now contain SIM cards that transmit their health status and equivalent body-monitoring for humans is already under trial. Cities like London and New York may even begin to "think" like organisms using smart roads and power grids. Not only will this data be of unimaginable size, it will be increasingly accessible from mobile devices that are ever more closely integrated with the human body and eventually the mind (Dragland, 2013).

For governments, this vastly increased knowledge is simultaneously viewed as an important economic driver and also a security panacea in an uncertain world. Whether security challenges are conceived in terms of traditional battlefield combat, insurgency, international terrorism, organised crime, peacekeeping or humanitarian relief operations, the common response has been to turn to knowledge-intensive organisations that increasingly deploy big data to manage risk (Amoore, 2011). As the majority of security threats have moved down the spectrum, so the focus of intelligence and security agencies had shifted towards human beings, as opposed to military hardware. Today, humans emit what the CIA has described as a constant stream of 'electronic exhaust fumes' as they live their lives (Zegart, 2007), and so intelligence sources can be as mundane as tweets, supermarket loyalty cards or gaming chat-rooms.

Although traditional human intelligence or 'espionage' will not become altogether redundant in the digital age – indeed, CIA assessments of Kremlin interference in the 2016 US election were derived from human sources in Russian cyber

outfits – big data is transforming the national security realm and opening the door to what we might call knowledge-intensive security. For example, the accessibility of large volumes of twitter feed raises the possibility of 'social media intelligence' in which scientists can seek to forecast future political trends across entire communities, cities or even countries. Could events like the Arab Spring have been forecast months ahead if the CIA had examined the twitter feed from Cairo or Tripoli in the right way? Scientists at MIT are convinced that they could. This sort of open source intelligence work looks less like traditional spying and more like the sort of large-scale behavioural research that academic sociologists longed to conduct in the 1970s, if only they had enjoyed access to enough data and computer power (Omand, 2015; Oh, Agrawal and Rao, 2013; Ruths and Pfeffer 2014).

The consequences of an intelligence world driven by big data are enormous and will take years, if not decades, to be fully understood. Yet, the implications for state secrecy are already revealing themselves. One of the fascinating features of this new landscape is the changing ownership of information. Unlike during the Cold War, secrets relating to security no longer belong to a few specialised government agencies and departments. Instead, they are dispersed throughout government, including local authorities and across business sub-contractors, partly because many of our new enemies are perceived to be within the 'homeland'. Moreover, private organisations including banks, airlines and ISP providers now collect, store, and share sensitive information relating to this sort of security on an unprecedented scale – often across state boundaries. Airlines and airports are good examples of "dual use" private intelligence partners, operating both as vast collectors but also customers of refined data for their own commercial and security purposes (Adey 2009).

Whistle-blowers and leakers thrive amid this new connected security activity. Edward Snowden is one of the clearest examples of this, sitting at a curious nexus between the state and the corporate and even between intelligence and information. A contractor for Dell and later Booz Hamilton, he extracted highly classified information not from NSA headquarters in Fort Meade, Maryland, but from a regional operations center 5,000 miles away in Hawaii, which he knew lacked adequate security software (Mazzetti and Schmidt, 2013). Indeed, unlike the internal secure network at Fort Meade, it has been claimed that the Hawaii office did not have the latest 'anti-leak software' because the area network bandwidth to the outpost was not enough for it be downloaded (Gallagher, 2013). If secret agencies can only do their business by plugging into Internet Service Providers and social media, their expectations of secrecy will necessarily have to be radically reduced.

Sharing Secrets

Government has itself done much to accelerate the present crisis of secrecy. The devastating 9/11 attacks were followed by a major cultural shift across the Anglospheric security community from the idea of "Need to Know" to a new mantra of "Need to Share" (Dawes et al, 2009). The most visible evidence of this was at Britain's technical intelligence agency GCHQ. Here, for almost half a century, intelligence work had been carried out on two sites dotted with fifty self-contained buildings that formed isolated security cells. Typically, the secretive civil servants that worked there might spend a twenty-year career in the unit that listened to the Soviet air force (J24) and so have little knowledge of what went on outside a single hut. Similar compartmentalization had also existed at Bletchley Park (Costas & Grey, 2016). In 2003, all this was replaced by "The

Doughnut", a vast circular building with a million square feet of office space that was for a while the largest building project in Europe. The most shocking thing for its new occupants was the open plan environment and hot-desking designed to encourage more interaction and a cultural 'change journey' within the organisation aimed at sharing widely (Crabb, 2005).

Meanwhile, in the US, investigations such as the 9/11 Commission had laid much of the blame for the attacks on vertical stove-piping and compartmentalized hoarding of information, which meant that the right information did not get in the right hands at the right time. Given the cross-border nature of terrorist and criminal networks, with threats living in the seams of national jurisdictions, the solution, they argued, was greater intra and cross-governmental connectivity. The order of the day became, 'play well with others'. However, it is now asserted by many national security practitioners that the recipe for correction went too far. Indeed, one State Department senior analyst has described what took place as 'an irrational exuberance of sharing' (Miller, 2011).

As a result of the newly enshrined emphasis on "Need to Share", security clearances were given to excessive numbers of people, including private contractors. In the US, 5.1 million people have clearances for access to classified information – roughly equivalent to the population of Norway and nearly rivalling the population of metropolitan Washington. (Fung, 2014). Elsewhere, it has been reported that a staggering 500,000 to 600,000 military and diplomatic personnel had access to the Pentagon's SIPRNet system that was used by Chelsea Manning, then a 22-year lowly Private First Class, to download a vast haul of classified material for onward dissemination to WikiLeaks (Sifry, 2011). Under political pressure to do more in the fight against global terrorism, government departments have been accused of following less than rigorous vetting procedures, routinely issuing 'interim clearances' based only

on self-disclosures to allow people to work on secret projects for months, sometimes years, without proper checks. In spring 2007, the then Under-Secretary of Defense Robert Andrews wrote a sobering memo to his superiors in which he claimed that 'Tens of thousands of people with classified access [have had] no comprehensive background investigation, creating an insider threat, the scope of which is unknown' (Eisler and Vanden Brook, 2013). In January 2013, the BBC revealed that some 27 UK Chief Police officers did not possess up-to-date security clearance, owing to stretched resources (BBC News, 2013).

In government, officials are only now waking up to the fact that, culturally, the expanded security workforce is very different to previous generations. Whereas working in the intelligence and security realm was once regarded as an honour and a privilege – CIA Director Richard Helms famously described it as a 'calling' – for many individuals today it is nothing more than a job, just like any other. Indeed, instead of building a career, many employees will join with every intention of staying only for a short time before moving on. Contractors are, by definition, nomadic. In this new revolving door environment, where security clearances at the Secret level are almost de rigueur, it stands to reason that there is not the same level of respect for traditional codes of secrecy. As privacy researcher Chris Soghioan has shown, many contractors will openly list their employment on classified programs on professional networking sites like LinkedIn, to enhance their employability (Swire, 2015: 5).

Contrary to the shrill observations of praetorian security chiefs, Snowden is not the cause of the present crisis of secrecy, but rather he is symptomatic of the structural changes that have led to it. Indeed, Snowden is emblematic of a new kind of operative who exists in the liminal space between public and private, fostered by advanced networking technologies and the development of e-government. These networks view

information sharing across traditional organizational boundaries as a primary virtue, seeking to use big data to address public needs that no single organization or jurisdiction can handle alone. But the work itself is far from glamorous and engenders little *esprit de corps*. Snowden was a community-college dropout who enlisted in the Army reserves only to wash out after 20 weeks, yet was privy to the innermost secrets of American intelligence gathering, working as a technician firstly for the CIA, where he left under a cloud, and then the NSA. United States Investigations Services Inc (USIS) – the contractor that screened Snowden – was investigated by the Justice Department for allegedly taking shortcuts when vetting federal employees. In August 2015, the company agreed to a settlement worth at least $30m (Hattem, 2015). In short, the rapid growth of "Need to Share" has introduced multiple failure points, the most important of which are cultural (Andrews Burrough and Ellison, 2014).

Computers and Counterculture

The structural changes in intelligence and security agencies since 9/11 are important and have undoubtedly rendered them more porous. No less important is an earlier decision by government to seek an alliance with the information and communications technology industry that has its roots in end of the Cold War. The termination of a conflict with the Soviet Union that had lasted almost half a century and which had given shape and purpose to national security confronted the intelligence agencies with multiple problems. Although politicians took their time in calling for a peace dividend, major agencies found their funding cut by about 25 per cent. Meanwhile, a globalizing world was presenting a bewildering range of new threats like non-state terrorism and

organised crime which, while not existential, required more resources, more languages, and more flexibility to track.

The biggest problem was the Internet itself. During the 1990s, the numbers of Internet users went from about four million to 361 million and the numbers of mobile phone users increased from sixteen million to 741 million (Aldrich, 2010: 486-7). In the 1980s email was an eccentric form of communications used by scientists in universities who wanted to chat online about quarks and quasars, but by 2002 the world was sending 31 billion emails a year. Fibre optic cables carried much of the traffic, but were difficult to tap into. Even if this tsunami of new electronic material could be collected and stored, analysing it seemed an impossible task. These required a broader range of skills and resources that were not available at that time to the relatively impecunious post-Cold War secret services (Aid, 2009).

The NSA and GCHQ were confronted with the need to address breath-taking changes in the realm of information and communications technologies just at the time when their own resource base had been cut. Looking for radical changes in working practises, they turned to the private sector. Partnerships with large companies like Narus and Northrup Grumman delivered innovative approaches that allowed NSA to trawl the Internet, providing what the agency called 'home field advantage' over terrorist groups. Meanwhile privatising many of NSA's logistical needs and back office functions allowed them to work a degree of budgetary magic. Booz Allen Hamilton was one of the major contractors that came to its assistance and one its employees was Edward Snowden. GCHQ moved down a similar path, with its mechanical engineering division (M Division) being entirely replaced by contracts to Vosper-Thorneycroft (Aldrich, 2010).

The 9/11 attacks and the invasion of Iraq accelerated this process of privatisation. Although these events are symbolic of intelligence failure, in their wake they nevertheless brought a massive influx of additional resources. Under President George W. Bush, the American intelligence community budget increased from $45 billion a year to $75 billion a year (Shane, 2012). This is almost certainly a profound underestimation since the operations in Iraq and Afghanistan brought with them additional moneys that helped to boost reconnaissance and surveillance programs (Belasco and Daggett, 2004). Again, the private sector was the source of increased capacity and by 2007, contracting constituted more than half the intelligence budget (Shorrock, 2007).

Retired NSA Director Michael Hayden believed that his alliance with the rising IT companies was the smartest thing he ever did (Hayden, 2016). However, he was strangely unaware of how ideologically antithetical some of his new allies were to traditional ideas of security and secrecy. The possibility of insecurity by IT contractors is not just about a change from legacy state employees to career-mobile contractors. Instead, it is about an entirely different view of the Internet as something that is alien to the realist world of international security and its agencies. Peter Swire, an eminent privacy lawyer who served on Obama's NSA review group in 2013, insists that this is signalled by the question of whether Snowden should be considered a traitor or a whistle-blower. During his work on the Review Group, Swire spoke with numerous people in the intelligence community. Not a single one said that Snowden was a whistle-blower, which in the US has positive connotations. The level of anger toward him was palpable. By contrast, a leader in a major Silicon Valley company said during the same period that more than 90 percent of his employees there would say that Snowden was a whistle-blower (Swire, 2015). The same ideological and generational

gulf could be detected between traditional print media and social media (Qin, 2015). Swire describes this as a sociological chasm and notes that NSA and other secret agencies face a formidable problem: how to guard secrets when much of the information technology talent has anti-secret and libertarian inclinations (Swire 2015).

The ire of Silicon Valley reached its peak after revelations about the physical subversion of the Internet. What has driven the technologists to distraction is increasing evidence that, over and beyond amassing data about ordinary citizens at a breath-taking pace (a largely passive activity), the agencies have been systematically undermining the security of the Internet and the software that the everyday citizen utilises. Anxious to appease Facebook's 1.6 billion global users, founder and CEO Mark Zuckerburg has publicly criticised calls from securocrats for the presence of so-called back-doors into its encryption technology, even hinting that an internet bill of rights should be created to preserve digital freedoms. In March 2017, Brad Smith, President of Microsoft joined him, describing government hacking as state attacks on civilians in peacetime and calling for a Digital Geneva Convention that would ban such practices. He argues that that these activities by NSA, GCHQ and their partners in countries such as Israel, are damaging to the fundamental fabric of democratic society and threatening to destabilise systems on which entire economies depend. While most scientists accept that nation states should have the authority to carry out targeted surveillance against obvious miscreants, they insist that it should not undermine the Internet's central place as a facilitator of free speech and innovation (Rogaway, 2015).

Those who privilege secure systems and a robust Internet enjoy increasingly powerful corporate allies. Large numbers of companies and individual computer users subscribe to protection from specialist online security companies such as AVG, Symantec, and Norton. These companies gather a great deal of data about network

activities, making it more difficult for government hackers to hide their trail. Typically, Symantec discovered that hundreds of hard drives had been compromised at source during their manufacture and were secretly pre-programmed to send their data back to Internet sink holes run by western intelligence agencies (Alrwais, 2016). Not only is this bad news for the perpetrators who hoped that their actions would remain secret for a long time, but also such activities provoke the technology community upon which they ultimately depend. These issues also beg the question of whether the Internet's heavy reliance on non-hierarchical, networked forms of governance is compatible with growing cyber-offence preparations by traditional state actors (Goode, 2015).

The Technology of Leaking

In September 1969, while working as a military analyst for the RAND Corporation in Santa Monica, California, Daniel Ellsberg came into possession of a secret Pentagon study of the Vietnam War. The history, which revealed that successive presidents from Harry Truman to Lyndon Johnson had repeatedly lied to the American people about the conflict, horrified Ellsberg and confirmed his belief that the conflict was both immoral and unwinnable. Believing that the public had a right to know, he put the first of the 47 volumes in his briefcase, prayed he would not be stopped by security guards, and ferried it to a small advertising company in West Hollywood, where there was a Xerox machine. ‘It was a big one, advanced for its time, but very slow by today’s standards’, he recalls (Ellsberg, 2003: 301). Night after night, for 18 months, he laboured to copy all 7,000 pages of the study, at ten cents a page, often getting home at dawn. Eventually, in late spring 1971, he passed copies of what became known as the “Pentagon Papers” to the *New York Times*. In the White House, Richard Nixon would later lament (in a

conversation, like many others, the disgraced 37th president generously taped for the historical record), 'we have the rocky situation where the sonofabitching thief is made a national hero and is going to get off on a mistrial. And the *New York Times* gets a Pulitzer Prize for stealing documents' (Ellsberg, 2003: 457).

Today, technology has advanced to the point where whistle-blowers no longer require all night sessions with a photocopier to steal classified material. For the national security state, IT has become a double-edged sword. On the one hand, positively, it has allowed for the collection and storage of huge quantities of information necessary for contemporary security and surveillance. On the other hand, negatively, it has undermined a central pillar of secrecy. At the start of the computer age, information was housed on isolated mainframes and if someone wanted to move it into the public domain, they would have to print it and somehow evade security guards. If the material was particularly voluminous (typically on the scale of the Manning or Snowden leaks), this was near impossible. Today, by contrast, enormous quantities of data reside on personal computers with connectors for a small copying device such as flash drives, rendering it much easier to pilfer information and avoid detection (Massey, 2013). Unlike in Ellsberg's day, when the only option for disseminating the material was going to the press or writing a memoir, leakers can now approach websites like WikiLeaks who, with anonymising software, will release it world-wide in a matter of seconds. Chelsea Manning smuggled 1.6 gigabytes of highly classified text files out of a US Army base in Iraq on rewritable compact discs – disguised as music by Lady Gaga – before downloading them onto a pen drive no longer than the length of a fingernail. Days later, the material was online, impossible for officials to retrieve.

The change to a mode of direct dissemination is important, since newspaper editors often constituted a middle way between openness and secrecy. When journalist

Dana Priest revealed the existence of secret prisons in three European countries in November 2005, officials persuaded her editors to delay the story and keep the identities of those countries a secret, to her obvious vexation (Priest, 2005). Even Snowden displayed a touching and old-school faith in traditional media, asking editors and journalists to decide which of his reported 200,000 documents should be released to the public and which should be held back in the cause of national security. Here too there was some uneasy negotiation between securocrats and editors. But increasingly, the temptation for leakers is to undertake a direct dump using anonymising software, not least because anything more complex might well result in prison or prolonged exile. Paradoxically, the use of intelligence methods to track down the sources of journalists makes disgruntled officials more likely to leak directly and indiscriminately via a website, avoiding interaction with the press.

While the Snowden revelations were accompanied by a moral panic focusing on the digital private lives of citizens, governments are also running scared of technology, at least from the perspective of protecting secrets. Highly-regarded computer security expert Bruce Schneier has predicted that just as efforts to stop file-sharing by the music and movie industries have failed, so will attempts to prevent the technology-enabled whistle-blower. Since 2010, a host of WikiLeaks imitators have burst forth onto the Internet, entice others to leak secrets. They include: BrusselsLeaks.com (focusing on the European Union); BalkanLeaks.eu (the Balkans); IndoLeaks.org (Indonesia); Rospil.info (Russia); GreekLeaks.org (environmental issues); and OpenLeaks.org, led by a number of former WikiLeaks employees (Sifry, 2011). Large news organizations are looking to create their own encrypted electronic drop boxes, giving would-be leakers the opportunity to submit sensitive material directly, thus cutting out problematic middlemen like Julian Assange. In 2011 *New York*

Times Executive Editor Bill Keller confirmed that the paper was discussing options for 'an EZ pass lane for leakers' (Calderone, 2011). For secret keepers, this conjures up the prospect of a journalism arms race to acquire large-scale leaks.

More fundamentally, technology is eroding the ability of states to do anything secretly. This is illustrated by the proliferation of commercial satellite imagery. Once the exclusive purview of government, in recent years, big technology companies have made giant strides in the development of high-resolution satellites and mapping applications, offering opportunities for global civil society to learn about secret geographical spaces, from espionage installations to nuclear facilities (Perkins & Dodge 2009). In 2009, the press in Pakistan published old Google Earth satellite photos showing American predators parked on the runway of a local airbase in 2006, thus confirming the US drone campaign in the country (Shachtman, 2009). In October 2012, Cryptome, a website dedicated to document disclosure from the national security sphere, posted pictures of a secret CIA training facility in Harvey Point, North Carolina, discovered on Bing Maps, which had served as the rehearsal site for the Navy SEAL raid on Osama Bin Laden (Cryptome, 2012). Most recently, in April 2017, a minute-by-minute log of a highly classified mission by a £650 million British spy plane near a Russian base on the Baltic Sea was recorded on a £2.99 mobile phone application called Flightradar24.com and shared widely on the Twittersphere (Nicol 2017). As cultural theorist Jack Bratich has argued, the growing availability of surveillance and imagery technologies on the open market has created the 'public secret sphere', where 'secrets' are 'spectacles' for public consumption (Bratich, 2007).

Conclusion

To speak of the 'end of secrecy' would be obvious hyperbole. Clearly, there will still be secrets and some things relating to national security will remain secret for a long time. Moreover, it is clear that governments are working hard to defeat transparency in the national security sector (Roberts, 2012). But the problem for government is that it no longer knows exactly how long it can keep things secret and this has a deterrent effect on future intelligence operations. For decades much of the CIA director's morning meeting was devoted to worrying about what had been said about the Agency in the morning editions. But in the past, the information emerging about their clandestine activities was often limited and sometimes even several decades old. As current secrets become known sooner, the cost of unsecrecy becomes ever higher. When deciding whether to approve an operation, intelligence chiefs have long pondered how their actions will appear if disclosed in tomorrow morning's newspapers. In the digital age, it is perhaps more accurate to think in terms of the 'Tweet test'; in other words, how will this look in ten minutes, on the Web, in 140 characters?

Governments are fighting back in a bid to offset this new reality. Increasingly, electronic programmes designed to profile government workers using algorithms tick away the background on government servers in an effort to identify "pre-leakers". Although Chelsea Manning's 35-year sentence was commuted by Obama in the final days of his presidency, she had still been imprisoned for 6 years and it is clear that intelligence agencies rely on the deterrent factor of lengthy prison sentences in their information assurance work. Yet the threat of incarceration alone is not sufficient. Increasingly, intelligence has moved away from a 'defensive' strategy of information control – i.e. saying nothing and releasing nothing – to a more 'forward' strategy that is designed to protect its reputation and promote public understanding of its work. We

have heard government public relations staffs talk about "nation-branding". Is it too adventurous to talk about efforts at "intelligence–branding" in the future? Some argue that this has been exemplified by the recent UK authorised histories of the Security Service and the Secret Intelligence Service and by the CIA's cooperation with the makers of *Zero Dark Thirty*, the Oscar-winning film about the hunt for bin Laden. In April 2014, the UK government announced the appointment of an official with a professional background in public relations as the new Director of GCHQ, Robert Hannigan (Moran, 2013; Quinn, 2014). All this is part of the new infosphere and we will need to develop new ideas around government attempts to manage public expectations in terms of declassification and openness.

Indeed, in the longer term, government will need to prepare for radical change triggered by Big Data. States increasingly claim that they need greater surveillance powers to prevent intelligence 'going dark' in the face of new forms of communications, but this is also a symptom of a shift away from intelligence towards information. We are moving into a new environment in which we need to think through the social implications of knowledge-intensive security. The Snowden episode signalled that intelligence is no longer owned by the intelligence agencies: instead it is owned by large corporations that are often multinational and in the future, it may even be owned by individual citizens with the skills to analyse large data sets. Indeed, there are already signs of this: the hunt for the Boston marathon bombers was aided in part by people on the Internet conducting their own crowd-sourcing of intelligence collection, piecing together cell-phone pictures and videos taken around the blast site by runners and spectators to form a picture of the suspects' movements. In this new realm of superabundant information, it may be that states will no longer "create" intelligence they will merely co-ordinate and "curate" intelligence. This is hardly

surprising given that Big Data is all about distributed networks, but the obvious corollary is that information will no longer a special badge for the initiates of an inner circle (Hall & Zarro, 2012).

Citizens will also need to prepare for greater transparency. The advent of a world in which everything around us gathers data means that individuals must expect for less privacy and corporations less confidentiality. Silicon Valley will need to reconcile its utopian belief in internet freedom and openness with its dogged determination to protect the privacy of its users. A portent of future troubles, Apple's refusal to hand over to the FBI encrypted information on an iPhone used by one of the San Bernandino shooters is an indication that cyber utopians want to have it both ways, as opponents of secrecy but also as advocates of privacy.

The challenge is clearly to ensure that knowledge-intensive security promotes a more open, prosperous and sustainable society. Increased transparency brings its own problems, but we are unlikely to be able to turn back the clock. Instead, we need to ensure that our data is owned openly, democratically and horizontally by everyone. We need to think hard about the growing role corporations will play, the ideas they espouse and what the implications are for democratic control over security. So far, Silicon Valley has understandably baulked at the prospect of any pact with government in which they are legally compelled to scan the private messages of their customers and report suspicious content. This dispute, and others like it, will become the norm and government attitudes to issues like publicly available encryption will become the litmus test of liberal and humane values. Ultimately, as we move into an era when the real world can be recorded and perhaps even manipulated in real time by those with the right software exploits, perhaps the decline of absolute secrets and their replacement with mere "delayed disclosure" is not unwelcome.

References

Adey, Peter. (2009) Facing airport security: affect, biopolitics, and the preemptive securitisation of the mobile body. *Environment and Planning D: Society and Space* 27(2), 274-295.

Aftergood, Steven. (2008) Reducing government secrecy: Finding what works. *Yale Law and Policy Review* 27(2), 399-416.

Aid, M.M. (2009) The Troubled Inheritance: The National Security Agency and the Obama Administration. in Johnson, L. (ed.) *The Oxford Handbook of National Security Intelligence.* Oxford: Oxford University Press, pp.243-56.

Aldrich, R.J. (2010) *GCHQ: The Untold Story of Britain's Most Secret Intelligence Agency.* London: HarperCollins.

Alrwais, S. et al. (2016) Catching predators at watering holes: finding and understanding strategically compromised websites. *Proceedings of the 32nd Annual Conference on Computer Security Applications*. ACM.

Amoore, L. (2011) Data derivatives: On the emergence of a security risk calculus for our times. *Theory, Culture & Society*, 28(6), 24-43.

Andrews, S., Burrough, B. and Ellison, S (2014) The Snowden Saga: A shadowland of secrets and light. *Vanity Fair* 18 (2014).

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., Walker, R.B.J. (2014) After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, 8(1), 121-144.

BBC News. (2013) Vetting of 27 UK Chief Police Officers Needs Updating. BBC, 23 January, http://www.bbc.co.uk/news/uk-england-20812559.

Belasco, A. and Daggett, S. (2004). *Congressional Research Report RL32422, The Administration's FY2005 Request for $25 Billion for Operations in Iraq and Afghanistan*, 22 July.

Born, H. and Leigh, I. (2005) *Making Intelligence Accountable: Legal Standards and Best Modes of Intelligence Surveillance.* Oslo: Parliament of Norway.

Bratich, J. (2007) Popular Secrecy and Occultural Studies. *Cultural Studies*, 21(1), 42-58.

Brevini, B., Hintz, A., and McCurdy P (eds) (2013) *Beyond WikiLeaks*. Basingstoke: Palgrave-Macmillan.

Calderone, N.M. (2011) New York Times Considers Creating EZ Pass Lane for Leakers. *The Cutline*, 25 January.

Coleman, E.G. and Golub, A. (2008) Hacker practice, moral genres and the cultural articulation of liberalism. *Anthropological Theory* 8(3), 255-277.

Costas, J. and Grey, C. (2016) *Secrecy at Work: The Hidden Architecture of Organizational Life*. Stanford: Stanford University Press.

Crabb, S. (2005) Out in the Open. *People Management*, 13 October.

Cryptome, (2012) Osama bin Laden Compound Raid Mock-up. 9 October. https://cryptome.org/2012-info/obl-raid-mockup/obl-raid-mockup.htm Accessed 12 December 2016.

Curtin, Deirdre (2014) Overseeing Secrets in the EU: A Democratic Perspective. *Journal of Common Market Studies*, 52(3), 1-17.

Dawes, S., Cresswell, A., and Pardo, T. (2009) From "need to know" to "need to share": Tangled problems, information boundaries, and the building of public sector knowledge networks. *Public Administration Review*, 69(3), 392-402.

Doyle, A., Lippert, R. and Lyon, D. (eds) (2012) *Eyes Everywhere: The Global Growth of Camera Surveillance.* London: Routledge.

Dragland, Å. (2013) 'Big Data, for better or worse: 90% of world's data generated over last two years'. *Science Daily*, 22 May.

Edgar, T.E. (2017) *Beyond Snowden: Privacy, Mass Surveillance and the Struggle to Reform the NSA.* Washington DC: Brookings Institution.

Eisler, P. and Vanden Brook, T. (2013) Security Clearances: Holes in the System? *USA Today*, 30 September.

Ellsberg, D. (2003) *Secrets: A Memoir of Vietnam and the Pentagon Papers.* New York: Penguin.

Fleitz, F.H. (2016) Should Congress Provide Safe Harbor to Intelligence Whistleblowers?, *International Journal of Intelligence and CounterIntelligence*, 29(3), 515-524.

Florini, A. (1998) The End of Secrecy. *Foreign Policy*, 7(1), 53-5.

Florini, A. (2004) Behind Closed Doors: Governmental Transparency Gives Way to Secrecy. *Harvard International Review* 26(1), 18-19.

Friedman, A. (2015) *My Way: Silvio Berlusconi*. London: Biteback.

Fuchs, C. (2015a) *Culture and Economy in the Age of Social Media*. New York: Routledge.

Fuchs, C. (2015b) Surveillance and Critical Theory. *Media and Communication*, 3(2), 6-9.

Fung, B. (2014) 5.1 million Americans have security clearances: That's more than the entire population of Norway. *Washington Post*, 24 March.

Gallagher, S. (2013) Snowden's NSA Post in Hawaii Failed to Install 'Anti-Leak' Software. *Arstechnica*, 18 October, https://arstechnica.com/tech-policy/2013/10/snowdens-nsa-post-in-hawaii-failed-to-install-anti-leak-software/

Gardner, L. (2016) *The War on Leakers: National Security and American Democracy, from Eugene V. Debs to Edward Snowden*. New York: New Press.

Garrett, K.R. (2006) Protest in an information society: A review of literature on social movements and new ICTs. *Information, Communication & Society*, 9(2), 202-224.

Gates, K.A. (2011) *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance.* New York: New York University Press.

Gibbs, D.N. (1995) Secrecy and International Relations. *Journal of Peace Research*, 32(1), 213–228.

Gibbs, D.N. (2011) Sigmund Freud as a theorist of government secrecy. in Maret, S. (ed.), *Government Secrecy*. New York: Emerald, pp.5–22.

Goode, I. (2015) Anonymous and the political ethos of hacktivism. *Popular Communication*, 13(1), 74-86.

Goold, B.J. (2004) *CCTV and Policing: Public Area Surveillance and Police Practices in Britain.* Oxford: Oxford University Press.

Greenwald, G. (2014) *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* London: Hamish Hamilton.

Gupta, A. (2008) Transparency under scrutiny: Information disclosure in global environmental governance. *Global Environmental Politics*, 8(2), 1-7.

Hall, C. and Zarro, M. (2012) Social curation on the website Pinterest.com. *Proceedings of the American Society for Information Science and Technology*, 49(1), 1–9.

Hansen, L. and Nissenbaum, H. (2009) Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53(4), 1155–1175.

Harding, L. (2014) *The Snowden Files.* London: Faber & Faber.

Harrison, M. (2013) Accounting for Secrets. *Journal of Economic History*, 73(4), 1008-40.

Hattem, J. (2015) Background Check Company that Screened Snowden to Forfeit $30m. *The Hill*, 20 August.

Hayden, M. (2016) *Playing to the Edge: American Intelligence in the Age of Terror*. New York: Random House.

Hintz, A. (2014) Outsourcing surveillance – Privatising policy: Communications regulation by commercial intermediaries. *Birkbeck Law Review*, 2 (2), 349-367.

Horn, E. (2011) Logics of political secrecy. *Theory, Culture & Society*, 28 (7), 103-22.

Johnson, L. (2014), An *INS* Special Forum: Implications of the Snowden Leaks. *Intelligence and National Security*, 29:6, 793-810.

Kelty, C. (2005) Geeks, social imaginaries, and recursive publics. *Cultural Anthropology* 20 (2), 185-214.

Leigh D. and Harding L. (2011) *WikiLeaks: Inside Julian Assange's War on Secrecy*. London: Public Affairs.

Lester, G. (2015) *When Should State Secrets Stay Secret? Accountability, Democratic Governance, and Intelligence*. Cambridge: Cambridge University Press.

Lyon, D. (2015a). *Surveillance after Snowden*. Cambridge: Polity.

Lyon, D. (2015b). The Snowden stakes: Challenges for understanding surveillance today. *Surveillance & Society*, 13 (2), 139-152.

Markham, C.J. (2014) Punishing the Publishing of Classified Materials: The Espionage Act and Wikileaks. *B.U. Public International Law Journal*, 23 (1).

Marx, Gary T., and Glenn W. Muschert. (2009) Simmel on secrecy in Cécile Rol, Christian Papilloud (eds.) *Soziologie als Möglichkeit*, Wiesbaden: VS Verlag für Sozialwissenschaften, pp.217-233.

Massey, L. (2013) Towards the End of Secrecy: Technological and Human Considerations. available at: http://bohr-conference2013.ku.dk/documents/papers/Massey_Towards_the_End_of_Secrecy_Technological_and_Human_Considerations.pdf.

Mazzetti, M. and Schmidt, M.S. (2013) Officials Say U.S. May Never Know Extent of Snowden's Leaks. *The New York Times*, 14 December.

McCraw, D. and Gikow, S. (2013) End to an Unspoken Bargain: National Security and Leaks in a Post-Pentagon Papers World. *The Harvard C.R.-C.L. L. Review*, 48(2), 473-509.

Miller, B.H. (2011) The Death of Secrecy: Need to Know…with Whom to Share. *Studies in Intelligence*, 55(3), 13-18.

Moran, C. (2013) *Classified: Secrecy and the State in Modern Britain*. Cambridge: Cambridge University Press.

Moran, C. and Aldrich, R.J. (2017) Trump and the CIA: Borrowing from Nixon's Playbook, *Foreign Affairs*, 24 April.

Moynihan, Daniel Patrick. (1999) *Secrecy: the American experience*. New Haven: Yale University Press.

Nicol, M. (2017) Plane Spotters with £2.99 app expose top secret UK spy plane off Russia, *Daily Mail*, 29 April 2017.

Oh, O., Agrawal, M. and Rao, H.R. (2013) Community intelligence and social media services: A rumor theoretic analysis of tweets during social crises. *Mis Quarterly*, 37(2), 407-426.

Perkins, C. and Dodge, M. (2009) Satellite Imagery and the Spectacle of Secret Spaces. *Geoforum*. 40(4), 546-560.

Phythian, M. (2007) The British Experience with Intelligence Accountability. *Intelligence and National Security*, 22(1), 75–99.

Pozen, David (2010) Deep Secrecy. *Stanford Law Review*, 62(2), 257-338.

Priest, D. (2005) Covert CIA Program Withstands New Furor. *The Washington Post*, 30 December.

Qin Jie (2015) Hero on Twitter, traitor on news: How social media and legacy news frame Snowden. *The International Journal of Press/Politics*, 20(2), 166-184.

Quinn, B. (2014) GCHQ Chief Accuses Tech Giants of Becoming Terrorists. 'Networks of Choice'. *Guardian*, 3 November.

Roberts, A. (2012) WikiLeaks: the illusion of transparency, *International Review of Administrative Sciences*, 78(1), 116-133.

Robertson, K.G. (1987) Intelligence, Terrorism and Civil Liberties, *Conflict Quarterly*, 7 (2), 43-62.

Rogaway, P. (2015) The Moral Character of Cryptographic Work. *IACR Cryptology ePrint Archive*, 1162-8.

Rourke, F.E. (1957) Secrecy in American Bureaucracy. *Political Science Quarterly*, 72: 540.

Rule, J.B. (2007) *Privacy in Peril.* Oxford: Oxford University Press.

Ruths, D. and Pfeffer, J. (2014) Social media for large studies of behaviour. *Science*, 346(6213), 1063-1064.

Sales, N.A. (2015) Can Technology Prevent Leaks. *Journal of National Security Law and Policy*, 8(1): 1-23

Schlesinger, A., Jr. (1987) Preface. In D. Banisar (ed.) *Government Secrecy: Decisions without Democracy*. Available at www.openthegovernment.com/org/govtsecrecy.pdf.

Schoenfeld, G. (2011) *Necessary secrets: national security, the media, and the rule of law*. New York: Norton.

Shachtman, N. (2009) Google Earth Shows U.S. Drones at Pakistani Air Base. *Wired* 19 February http://cryptome.org/2012-info/obl-raid-mockup/obl-raid-mockup.htm

Shane, S. (2012) Cost to Protect U.S. Secrets Doubles to Over $11 Billion. *The New York Times*, 21 February.

Shorrock, T. (2008) *Spies for Hire: The Secret World of Intelligence Outsourcing*. New York. Simon and Schuster.

Sifry, M.L. (2011) In the Age of WikiLeaks, the End of Secrecy? *The Nation*, 3 March.

Swire, P. (2015) The Declining Half-Life of Secrets, *New America Cybersecurity Fellows Paper* - Number 1 https://static.newamerica.org/attachments/4425-the-declining-half-life-of-secrets/

Theoharis, A. (2016) Expanding US Surveillance Powers: The Costs of Secrecy', *Journal of Policy History*, 28(3), 515-534.

Thomson, P. (2015) Secret Canberra: Security Vetting Costs Millions as Public Service Job Freeze Thaws. *The Canberra Times*, 1 April.

Van Buren, P. (2012) Obama's Unprecedented War on Whistleblowers. *Salon*, 9 February.

Vincent, D. (2016) *Privacy: A Short History.* Cambridge: Polity Press.

Watts, N. (2012) David Davis says case for secret courts based on a 'falsehood'. *Guardian*, 15 May.

Max Weber, (1918) *Wirtschaft und Gesellschaft*, ix/2, 730-31.

Wicker, S. (2013) *Cellular Convergence and the Death of Privacy*. New York: Oxford University Press.

Zegart, A. (2007) *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Princeton: Princeton University Press.