*Information & Security: An International Journal*

Peter Gill, vol.30, 2013, 11-28 http://dx.doi.org/10.11610/isij.3001

# SHOULD THE INTELLIGENCE AGENCIES 'SHOW MORE LEG' OR HAVE THEY JUST BEEN STRIPPED NAKED? [1]

Peter GILL

**Abstract:** Newspapers started publishing US National Security Agency (NSA) files in June 2013, as a result of Edward Snowden's declaration that he wanted to start a debate on the current drive for 'total surveillance.' Official comments in the UK have been tight-lipped and have barely got beyond the refrain that everything NSA's sister agency, UK Government Communications Headquarters (GCHQ) does is legal and requires no further discussion. This article considers the major issues that have been raised concerning privacy, surveillance and the adequacy or otherwise of political control and oversight over intelligence agencies, particularly in the UK.

**Keywords:** Intelligence, surveillance, privacy, oversight, human rights, data mining, profiling.

## Introduction

When Edward Snowden gave his first interview in Hong Kong in June 2013, having flown there from his home and work in Hawaii and in possession of 58,000 highly classified NSA documents,[2] he said

> I really want the focus to be on these documents and the debate which I hope this will trigger among citizens around the globe about what kind of world we want to live in… I can't allow the US Government to destroy privacy, internet freedom and basic liberties… My sole motive is to inform the public as to that which is done in their name and that which is done against them.[3]

In the subsequent four months he appears to have been very successful since US officials from the President down have acknowledged the need for some greater public consideration of the issues involved[4] amid, no doubt, much private grinding of teeth and cursing. Debate in the UK has been more muted because most of the UK media acceded to a Defence Advisory notice from the Government asking them not to give further publicity to the Guardian's disclosures.[5] Official comments in the UK have

been, typically, much more tight-lipped and have barely got beyond the refrain that everything GCHQ does is legal, subject to control and oversight, and thus requires no further discussion.[6] But, clearly, major issues relating to privacy, surveillance and the adequacy or otherwise of political controls over intelligence agencies have been raised and this article considers the implications of the published documents in the prevailing context of legal and political oversight in the UK. Its own SIGINT agency, GCHQ, has figured largely in the revelations because of its long-standing and close relationship with NSA.[7] There is no detailed consideration of the related debates as to the wisdom or not of newspapers publishing the documents.

So, what is the problem? What realistic expectations of privacy can we have in the context of rapidly evolving technology, antiquated legal structures, massive and intrusive tracking by private corporations and widespread volunteering of personal information via social media? [8] Millions of people now carry on their person a device, the smartphone, by which their movements can be immediately tracked and their telephone calls and Internet activity logged. Extensive surveillance of this activity is carried out by the private corporations whose services we sign up for—Google, Microsoft, etc.—but we do not thereby also grant permission to states also to hoover this up. There are certain human rights which states may not infringe in any circumstances, for example, torture, or only in a declared state of emergency, such as detention without trial, but privacy is one of those rights that states may infringe *at any time* in the interests of national security, public health and safety. Although intelligence services rely to some extent on the collection of open source material, what is distinctive about them compared to other public bodies is their possession of special legal powers and technologies that enable covert surveillance. To be legal, this requires proper authorisation (the mechanism varies between countries, in some it will be judicial, in others, such as UK, ministerial); it must be necessary because the information is unavailable otherwise, and the means must be proportional to the objective, for example, to gather information relevant to the prevention of a violent attack or illegal trafficking. Does this include the mass surveillance of communications such as revealed in the Snowden documents?

Recent commentary on the NSA files indicates broad acceptance of the principle that states may target for surveillance when there are grounds for suspecting some involvement but there is great unease at the apparent threat posed by state surveillance of *all* communications. Is this a new problem or have we been asleep for years while intelligence agencies quietly gathered all there was to know about us? Briefly, while the state always assumed the prerogative power to intercept communications since technologies developed beyond personal contact, that is, the postal services in early 17th century and telegraph/telephone in late 19th century, this was subject to no external check, although the procedure by which ministers would sign warrants was regu-

larised in the 1950s. This changed after the European Court of Human Rights (ECtHR) found for James Malone[9] in 1984 and declared the necessity for a statute setting out the circumstances under which telephone tapping might take place, and appropriate mechanisms both for checking the legality of authorisations and by which the public might complain if they believed their rights had been wrongly infringed. Under the 1985 Interception of Communications Act (IOCA) which outlawed interception without a ministerial warrant, therefore, the Interception of Communications Commissioner (ICC) would report each year on the findings of the *post hoc* review of the legality of any authorisation and would provide some indication of the numbers of warrants given under certain headings but not others. However, either listening to conversations 'in real time' or taping them and having them transcribed (including, possibly, translation) was a very expensive business in terms of time and money. Many investigations, therefore, would make use of what was then called 'metering' information—the record of outgoing and incoming numbers and call duration—that would be analysed in order to build up a map of the networks involved in targeted activities. No warrant was required for agencies to obtain this data from communications providers – they just asked communications providers for it.

Intelligence logic is aimed at trying to prevent bad things happening and therefore, given the essential unknowability of the future, has always lent towards the collection of as much information as possible ("you never know today what you might need tomorrow…") even if it was based on a false empiricist logic that more data would lead to a conclusion. Therefore, the exponential increases in information and communications technologies (ICT) during the last twenty years have started to fulfil the dreams of security officials to be able to 'collect' and potentially 'know' everything. These developments coincided broadly with a radical shift in some governments', notably the U.S. and UK, perception of threats.

Intelligence played a major part in preventing the Cold War between US and USSR getting hot (though there were many proxy wars in Asia and Africa) by succeeding in informing political leaderships well enough as to the capabilities of each other that no-one wanted to risk the 'mutually assured destruction' that would result from armed conflict. There was less certainty as to the precise intentions of each side but, in general, they were at least rationally calculable. But 9/11 signalled a major shift: al Qaeda's intentions seemed clear—to kill as many people as possible—while there was much more uncertainty as to their capabilities and internal security services found themselves struggling to identify those who were potentially violent. For a decade after 9/11, MI5 struggled to work out how many potential terrorists there were, where they lived, and what capabilities they had. Believers in jihad were many but the process by which a few might actually plan to carry out violent attacks was disconcertingly rapid.[10] There were many consequences of this changed threat environment,

hence one was to increase the demand for more widespread surveillance of all types, human and technical, in order to try to reduce the uncertainty which, at times, approximated ignorance with the concomitant risk of over-reaction. This demand was both professional and political: after the Iraq intelligence fiasco and the 'failures' to prevent 9/11 and 7/7, security professionals had a natural desire to up their game while, for politicians, the risks were high if they were not seen to be doing all they could to prevent attacks and keep the public safe. The precautionary principle was to be applied to counter-terrorism[11] and intelligence was to shift from 'gathering' to 'hunting.'[12] On the other side of the equation, as demand for increased surveillance grew so did the array of companies, large and small, who would be prepared to supply and assist in the development of ever more sophisticated means of processing information. Thus the integration of states and corporations was intensified but it was never complete: when companies could not or would not comply, we learn, the US may conduct an 'off-net operation' in which clandestine CIA operators will plant spying software in computer servers and data switching centres in order to facilitate NSA surveillance that could not be initiated remotely.[13]

But, as far as communications are concerned, the 'big idea' since 9/11 was the 'mining' of 'data warehouses' constructed by linking public and private databases. This has been made technically possible by XML (Extended Markup Language) software that enables previously separate databases to be 'merged' *via* a universal language and mining "involves the use of sophisticated data analysis tools to discover previously unknown, valid patterns and relationships in large data sets."[14] Some of the examples in the security field are truly awesome: inspired by the conclusion that in the period before 9/11 there was a failure within the US intelligence and law enforcement communities to 'join the dots'[15] between items of information already in the system, major efforts have been underway to seek solutions. For example, in a report commended by the 9/11 Commission, the Markle Foundation proposed a Systemwide Homeland Analysis and Resource Exchange (SHARE) Network that would enable information sharing by federal, state, local government and private sector users.[16] Subsequently, the Department of Homeland Security (DHS) funded a study carried out by the U.S. National Research Council which noted the undoubted success of automated data mining in commercial settings, for example, in detecting fraud, but concluded that it was neither feasible nor desirable for the identification of terrorists. It also argued that behavioural observation and physiological monitoring should only be used to identify individuals for follow-up checks because of the risk of false positives and vulnerability to countermeasures.[17] The NSA files now published tell us more about the development of data mining.

## Targeting the knowns and searching for the unknowns

In the broadest sense, there are two issues for intelligence agencies seeking to prevent attacks: tracking the communications of those who are known or suspected of involvement and searching communications for evidence of activities by those who are currently unknown.[18] UK law authorising the first is well understood: warrants[19] will be signed by ministers and be subject to subsequent review by the ICC. Technically, of course, things have become much more complicated in the last quarter century as means of communication have proliferated – landlines, mobile telephones, text messaging, Internet-based e-mail, websites, chat rooms, social networking and so on. Therefore, even if specific names have been targeted, much searching of radio, satellite and cable communications may be necessary in order to locate specific communications made or received by a targeted person. This kind of searching will usually start by accessing 'metadata' or communications data, which is the modern equivalent of the metering information discussed above. UK agencies do not need a warrant to access meta or communications data (RIPA ss21-25; the US equivalent is the Patriot Act s.215). This is still used to establish who is communicating with whom, from where and by what means etc., and is still quicker and cheaper to access, if less useful than content, but whereas it used to be the case that it was arguably less intrusive on an individual's privacy, this is now widely doubted. Metadata in some cases will be transmitted as part of the communication content, for example, where someone uses a third party communications provider hosted on her CSP, details of the final recipient will be held within the content of the data packet.[20] But all of this assumes that the name of the target is known. What of people who may be involved in 'threatening activities' but whose identity is not yet known? This is where the current controversies really take off.

The question of how targets for surveillance are identified is critical because, although the *potential* for total surveillance now appears to exist, it remains an unrealisable dream for securocrats with a totalitarian streak while remaining a nightmare for the rest of us. The contest between surveillance and counter-measures is constant, resembling a classic arms race. Targeting everywhere is ultimately defined by political priorities and legal requirements. In totalitarian or authoritarian regimes the former rules and people will be subject to surveillance if they are perceived as 'enemies' of the regime. One of the key elements of the 'democratisation' of former authoritarian regimes in Eastern Europe and Latin America during the last thirty or so years is the passage of statutes which bring intelligence within the rule of law. Typically, these laws set out the mandate for the agencies in terms of threats to national security, enumerate the special powers they have to collect and process information, establish some procedure by which their exercise must be authorised and erect some oversight system. Such laws provide the basic requirement for democratic governance of intel-

ligence but their practical impact varies greatly, and this includes the 'old' democracies who also established clearer legal frameworks for intelligence during this period.

But, despite the increase in formal law underlying intelligence targeting, it remains crucial to study intelligence policies and practices. Until twenty years ago, intelligence methods had remained essentially unchanged for millennia: agencies would seek to identify and then surveil targets by some combination of human and technical means. Names of potential targets would be generated from 'information received,' meetings attended, publications read, bookshops visited, petitions copied or from partner agencies but, most often, the resulting 'record' would consist of no more than an index card. In some cases a file would be opened and more active investigative measures be taken: existing informers be tasked to find out more, telephone records consulted or, in some cases, calls intercepted. But the numbers of active targets at any one time was never that high; more frequent was that a file would be added to as and when information came in from longstanding technical (telephone taps) or human (informers) sources.

The new communications technologies held out the prospect of radical shifts in two ways. First, the capacity for collection, processing and storage of masses of communications data increased the numbers of individual targets on whom information could be more actively gathered at any one time. However, it did not necessarily follow that this increased the effectiveness of agencies since the increase in ability to store information was not matched by an increase in the ability to analyse what it all meant or, necessarily, to take any action if it were warranted. The communications revolution did not change the basic fact that even a targeted intercept (under IOCA 3[1]) might carefully record "two idiots speaking on the phone."

Second, and more fundamentally, the new technologies held out greater promise of identifying those currently 'unknown.' Targeting an individual for telephone interception thirty years ago would, certainly, also incidentally overhear the conversations of other people using the same telephone but there was no general surveillance of telephone conversations, at least until they started travelling 'wirelessly' via radio and satellite connections. We learned from the reports of the Echelon system in the 1990s that transatlantic satellite communications would be searched by means of a 'dictionary' of keywords so that the messages containing them could be further interrogated.[21] This was a case in which the technologies of surveillance appeared to have outstretched the prevailing law but perhaps not. IOCA, in addition to the warrant procedure identifying specific names and addresses (3[1]), provided a much more general power in the following sub-section:

> 3(2) Subsection (1) above shall not apply to a warrant if –
> (a) the interception required by a warrant is the interception, in the course of their

> transmission by means of a public communication system, of –
>
> (i) such *external communications as are described in the warrant*; and
>
> (ii) such other communications (if any) as it is necessary to intercept in order to intercept such external communications as are so described; and
>
> (b) at the time when the warrant is issued, the Secretary of State issues a certificate *certifying the descriptions of intercepted material* the examination of which he considers necessary (in the interests of national security; for the purpose of preventing and detecting serious crime; or for the purpose of safeguarding the economic well-being of the United Kingdom).[22]

Now, the limitation of this *general* interception to external communications (those involving someone outside the country) was much more significant in the mid-1980s than it is now, when it has no significance; we must remember that, then as now, GCHQ was tightly bound within UKUSA in which US, UK, Australia, Canada and New Zealand cooperated to share collection and product so as to achieve global coverage of communications. So, to the extent that GCHQ's contribution was defined as the collection of communications involving some foreign party and the minister had signed the relevant certificated warrant 'describing' the targeted communications, the letter of the law was satisfied. Some commentators on IOCA noted that this legalised 'trawling'[23] but whether this was fully understood, let alone supported, by people outside the securocracy is another matter.

A combination of rapid data processing and new 'relational' software meant that data banks could be searched to identify names, contact addresses etc. based on some 'profile' of suspicious activity, travel or financial pattern. The Dutch Review Committee on the Intelligence and Security Services (RCISS) has provided a useful explanation of why and how this works. What they call 'generic identities' cover a particular 'type' of person or organisation and obviate the need for identifying specific individuals. The advantages for the agencies are obvious: the specific names and locations of individuals may not be known, organisations change their names, people use aliases and so on.[24] But there are problems with this, even from the agency perspective: the more broadly the profile or 'generic identity' is drawn, the higher the number of communications selected and the greater the time and the resources required to 'weed out' those who should not be targets – false positives. On the other hand, the narrower the construction of any profile, the greater the chances that someone who should be targeted might be left out – the problem of false negatives. From the privacy perspective, the dangers of profiling are clear: many people may be subject to privacy intrusions or worse and, in practice, it may not get beyond ethnic or racial profiling.

When the 1998 Human Rights Act (HRA) was passed, meaning that the ECHR would be applicable by UK courts, the need was felt to 'protect' intelligence gathering from court challenges by ensuring that the regime for authorisation and oversight would

pass muster before the ECtHR. So, two years later, when the HRA became effective, the Regulation of Investigatory Powers Act (RIPA) also became law and codified the information gathering powers of the state. This retained the essential distinction between a warrant for interception of named people and places under s.8(1) and a 'certificated' warrant under 8(4).[25] In other words, by 9/11, as far as the security authorities were concerned, the legal framework to support the enhanced significance of data mining was already in place and, despite the interest in the European Parliament in Echelon, was essentially uncontested. It is the same confidence in the all-encompassing nature of the UK legal framework that no doubt led former GCHQ Director David Omand to argue that "For Britain, Snowden's public interest justification is thin since subsequent investigation has shown conclusively (that GCHQ) has at all times acted lawfully."[26] This reassurance is somewhat lessened, however, by the evidence that one of GCHQ's 'key selling points' in its financially subsidised relationship with NSA is the UK's more relaxed legal regime.[27]

## The Snowden files: what do they tell us?

Snowden has now provided much information to fill the gaps in our understanding of the mechanics of this surveillance. Apparently the NSA's PRISM programme relies on collecting directly from the servers of providers such as Microsoft, Google and Facebook. Reportedly, this had almost 120K active surveillance targets in the database as of April 2013 with analysts required to have 51 % confidence that the target is a foreign national not in the US at the time of collection.[28] The cooperation of foreign-owned communications companies can be ensured by making their licences dependent on signing a 'network security agreement' that requires them to have a centre for handling surveillance requests on US soil, staffed by cleared US citizens.[29] James Bamford has described how on entering a communications service provider (CSP) facility the fibre optic cables go into a 'beam-splitter' that produces a mirror image of the original communication. The original travels on while the duplicate enters the NSA room and is scanned for 'selectors' with any selected messages being re-transmitted to NSA.[30]

Since the communications infrastructure is largely in private hands, the costs of interception are much reduced if the CSPs cooperate. However, not all do and there is a second programme—'Upstream'—for the collection of data directly from fibre cables or computing infrastructure. NSA has been constructing a new facility in Utah for the storage and analysis of everything collected.[31] GCHQ also collects material from the cables as they come ashore from the Atlantic in an operation named 'Temporaл' Thirty percent of the massive volume of communications is immediately rejected while 40,000 'selectors' chosen by GCHQ and 31,000 by NSA based on key words, phone numbers etc. trawl the rest. A programme called TINT then facilitates storage

permitting retrospective analysis by the 300 GCHQ and 250 NSA analysts working on 'target discovery' and 'target development.'[32] 1–2 billion records a day are collected, content remains on the system for 3-5 days and metadata is stored for 30 days though analysts can store 'interesting' material in another database for up to five years.[33] In a public statement challenging a press story as to the extent of NSA surveillance, the NSA and ODNI said that, using all its authorities, the agency 'touches' 1.6 % of internet traffic and that analysts 'look at' 0.00004 %.[34] Although the agencies have not earned a reputation for complete openness in recent months, these figures look plausible: if 2 billion records a day are 'collected,' the 1.6 % that are 'selected' amount to 32 million, which far exceeds anything that could realistically be 'analysed.' So, about 80,000 will be 'looked at' which sounds barely plausible if one accepts that 'analysis,' however clever the software in use, ultimately requires a human being to decide what the communication means. For certain, this facility has not solved the problem of 'overload.'

But after collection the next big challenge for the agencies is the ubiquity of encryption. RIPA attempted to deal with this in Part III whereby CSPs could be required to supply information in uncoded form or to supply the key required to 'unlock' it and could face criminal sanctions for non-compliance and for disclosing the fact that a disclosure notice had been served.[35] But this relatively uncontroversial legal compliance by the CSPs has been compounded by one of the most closely guarded secrets of all so far revealed by Snowden's data which is the collaboration between the agencies and the CSPs to provide backdoors or trapdoors into their software. Here although the companies deny that they cooperate in this way, the motivation of the companies is presumably a mix of the patriotic and the financial.[36]

But what happens when there is no compliant CSP to provide the key? More than a year before Snowden's departure from Hawaii, Bamford described how the NSA's new computer behemoth in Utah was partly designed in order to create the sheer computing power that would be needed to attack the Advanced Encryption Standard now incorporated in most commercial email programmes, web browsers and, indeed, as is used by the USG for top secret communications. Building on the success of the US Department of Energy in constructing the world's fastest computer by 2009, NSA built an even faster one that was customised specifically for cryptanalysis and was believed to be on the verge of unlocking many years of stored data.[37] GCHQ, too, is engaged in trying to ensure that it can keep pace with encryption so that the ability to understand the flow of information it collects from accessing cables does not degrade. Apart from seeking to 'crack' codes through computing power, GCHQ also deployed a Humint Operations Team which was responsible for recruiting and running covert agents within CSPs who could provide useful intelligence.[38]

Although the search for total surveillance would seem to be almost in reach, some targets are much harder than others: foreign governments, military organisations, and large corporations all seek to protect their communications more carefully than even the most privacy-conscious citizen (and have the means to do it). Tor ('the onion router'), for example, is an open source public project used by many to safeguard their on-line anonymity, including dissidents in repressive regimes but also, no doubt, criminals, and has still resisted attempts by the agencies to compromise its core security.[39] There has been much criticism of the agencies attack on encryption including the insertion of backdoors into commercial software because, it is argued, it renders the software more vulnerable to other hackers and threatens its integrity for all computer users.[40]

Most of the implications of the leaked NSA files concern the *defensive* aspect of surveillance—seeking to locate threats in time to disrupt them—and NSA Director, General Keith Alexander argued to the US Senate that 'dozens' of plots had been foiled in part because of the domestic surveillance dragnet…' The FBI cited two cases, one involving people sending money to *al Shabab* in Somalia, the other the plot to bomb NY stock exchange (though in latter there had been no trial).[41] It has been argued that both cases depended on 'traditional' surveillance of known numbers rather than the mass vacuuming up of communications data.[42] Clearly, one of the great problems in assessing the effectiveness of any intelligence technique is that evidence may be unavailable, at least to outsiders.

But there has been far less discussion of the *offensive* aspect to surveillance which has been institutionalised in the U.S. in the form of Cyber Command which deploys about 4000 people, some defensively but also offensively, as in the disruption of the Iranian nuclear programme in 2009 by means of the Stuxnet worm which was developed by NSA and its Israeli counterpart. In 2011, according to budget documents, there were a total of 231 offensive cyber operations which can include alterations of data, turning off networks, and establishing a presence inside systems for subsequent exploitation.[43] A different type of attack occurred on September 11, 2008 when the US Joint Special Operations Command shut down all the jihadist web-sites they knew of.[44]

Debate will doubtless go on for a long time as to the damage, if any, done by Snowden's disclosures. David Omand, as we saw at the beginning, is in no doubt that this could be very serious. He observes that materials 'stolen' by Snowden might now be in hands of China and Russian intelligence services which could lead to lines of intelligence drying up and cyber-attackers learning how to avoid defences and that damage to security could have been done because journalists are not best placed to know where material might fit into adversaries' jigsaw puzzles.[45] US officials have noted no immediate impact of Snowden's disclosures on levels of electronic communication but express similar fears to Omand's as to the potential longer term impact of

the disclosures.[46] In a public speech on October 8, Andrew Parker, MI5 Director referred to the 'margin of advantage' that the agencies have through the capabilities they use against terrorists and said: "It causes enormous damage to make public the reach and limits of GCHQ techniques. Such information hands the advantage to the terrorists."[47]

## The challenge of total surveillance and the need for better control and oversight

Technologies of communications and surveillance are *always* ahead of the law and regulation. No government will deny itself the opportunity to increase surveillance, therefore the laws in relation to privacy *always* lag behind. The complexities involved in contemporary communications and surveillance are such that they are *never* understood by (non-expert) regulators or overseers. Therefore Index on Censorship's petition calling on government leaders to "clearly and unambiguously state their opposition to all systems of mass surveillance including the Prism system" will go unheard. Some individual leaders may voice concern or criticism, such as Dilma Roussef at the UN in protest at NSA monitoring her phone calls[48] but that will be to satisfy domestic opposition rather than reflect what their governments actually want.

An initial move in the U.S. House of Representatives to block funding for NSA mass rather than targeted surveillance was defeated narrowly on July 24 but 11 new reforms were being considered in Congress by early August.[49] Whether any of these get beyond the stage of symbolic politics remains to be seen. A bipartisan measure was introduced by four senators on September 25 but the proposal seeks to limit NSA mass surveillance of communications data and the Internet only insofar as it affects US citizens.[50]

Can the law be redrawn for more specificity so that surveillance could only be triggered by evidence of pending illegality, as argued by Paddy Ashdown?[51] Well, it could be by simply deleting s.8(4) from RIPA but it is difficult to imagine any government agreeing to this. More generally, history shows that governments always draw up security legislation in the broadest terms that their domestic political context allows so as to maximise their room for discretion and to deal with future circumstances that they fear but cannot predict. It has proven impossible to have government in UK limit what it might do in the security field voluntarily by law. Laws will abide by the ECHR but as long as there is an authorisation process and some minimal review mechanism surveillance is effectively unhampered. It will be interesting to see what happens to Privacy International's complaint filed with the UK Investigatory Powers Tribunal, arguing that Tempora is breach of ECHR, and the similar case filed by NGOs at the ECtHR alleging that internet trawling is illegal.[52]

'Oversight' refers to the review or scrutiny of intelligence activities so that those directing them can be held accountable. The main objective of the scrutiny is to secure public trust in the agencies through ensuring that their expenditure is efficient and effective and that their operations are legal with proper respect for human rights. This scrutiny will, ideally, be carried out both by specialist units *within* agencies and ministries as well as externally by parliamentary and/or extra-parliamentary bodies.

There are particular problems inherent in intelligence oversight everywhere. Foremost is the secrecy within which intelligence operates. In some respects there is more openness now about intelligence than there was during the Cold War; for example, UK governments denied the very existence of MI6 in peacetime and until the 1980s there simply was no external oversight of intelligence in the UK. Yet the agencies are especially concerned to safeguard their 'sources and methods' for fear that, if they are revealed, operations will be compromised and, in the case of human sources, possibly killed. But while this secrecy is justified, it can facilitate abuse of power, inefficiency or corruption. In response to the steady stream of revelations showing the extent to which U.S. congress and public has been misled about the extent of surveillance, especially of U.S. citizens, Senator Ron Wyden, member of Senate intelligence committee has described the 'culture of misinformation' inside US agencies, directed not just at adversaries but also at public and legislative overseers.[53] In the wake of these revelations, a number of previously classified FISA (Foreign Intelligence Surveillance Act) judgments have been made public and in a 2011 decision, Judge John Bates noted that it was the third time in as many years that the NSA had disclosed "a substantial misrepresentation regarding the scope of a major collection programme."[54]

Second, matters of national security and public safety are the central concern of any democratic government and consequently intelligence agencies are close to the heart of political power. This brings an ever-present danger of intelligence being politicised; rather than 'speaking truth unto power,' agencies may tell politicians what they wish to hear or act in their partisan interest by surveilling opponents.[55] In the wake of Snowden's disclosures Michael Hayden, former director both of NSA (1999-2005) and CIA (2006-2009) argued in a speech in London that U.S. and UK agencies would have 'to show a lot more leg' if they wanted to win broad public understanding and support for the kind of surveillance programmes they were undertaking.[56]

When Snowden's material first appeared in June 2013, William Hague, the Foreign Secretary, and thus responsible for GCHQ, sought to reassure Parliament that the UK agencies work within "the strongest system of checks and balances for secret intelligence anywhere in the world."[57] The most public part of the UK oversight architecture is the Intelligence and Security Committee (ISC)[58] which was established as a 'committee of parliamentarians' in 1994. It received generally favourable reviews of

its performance until 2003[59] but thereafter its poor performance over Iraqi weapons of mass destruction, the abuse of detainees in Afghanistan and Iraq and extraordinary rendition tarnished its reputation. However, its Chair, Malcolm Rifkind, in wake of Snowden's revelations, observed that ISC is now more empowered as a result of changes to its mandate in the Justice and Security Act 2012, has almost twice the budget and a strengthened staff and claimed that it is part of the most effective and independent oversight system in the world.[60]

But the weakness of the current UK structure including the ISC and the ICC can be seen from their reaction to the Government's proposed Communications Data Bill in 2012. This was intended to up-date powers to intercept communications to the age of social networks and Skype but, in the context of Snowden's revelations, it is clear that the Government was essentially seeking additional powers to oblige private companies to cooperate with GCHQ. Anyway, the ISC inquired into the specific impact on the security and intelligence agencies, publishing its report in February 2013. The report is interesting as to the alleged gap in the 'capability' of agencies to access communications data, and how the government could require, if appropriately authorised, CSPs to apply Deep Packet Inspection probes into their networks to collect the required information. However, there was no mention of the mass collection of data for the purposes of data mining. Similarly, the ICC reported that 3,372 'lawful intercept warrants' were issued in 2012 but we were not told how many of those were under 8(1) and how many under 8(4). The Report shows the detailed process by which 8(1) warrants in relation to names/places are obtained but says nothing about the more general warrants.[61] Why is the distinction not discussed? It is inconceivable that the ICC is unaware of them but are they examined? If so, why are they not discussed in the public report – is this a case of not wishing to frighten the children? ISC and the ICC may well protest that their failure to discuss data mining was to preserve the integrity of intelligence methods but there had been enough discussion of the issue pre-Snowden that *some* official contribution would have been appropriate to educate and reassure (or not) the public.

Some weeks after the Snowden material started appearing, the ISC issued a brief statement including a one-line dismissal of GCHQ data mining via PRISM which was clearly inadequate and did not even refer to GCHQ's own 'Tempora' programme.[62] This might be contrasted with RCISS informed and balanced discussion of the specific legal and policy implications of targeted interception compared with 'trawling' provided by the Dutch review Committee. The ISC may now have more powers and staff but it is structurally flawed. MPs are too busy to provide the necessary research and monitoring. Perhaps stung by criticism of its initially inadequate reaction to the Snowden disclosures, the ISC announced on October 17 that it would conduct a wider inquiry into the UK legal framework and the impact of mass surveillance on people's

privacy. They would also hold some public evidence sessions; so, even in the UK, Edward Snowden may be getting his debate.

## Conclusion

Thirty years ago intelligence and surveillance were easier to comprehend: they were targeted at individuals and groups and criticism could be made if these processes led to the wrongful surveillance or arrest/imprisonment of those who were actually innocent. There was no total surveillance though, in authoritarian states, the net would be cast very wide and cause much misery since any dissent was interpreted as the subversive acts of 'enemies of the state and the people.' There were some similar problems in liberal democracies but they were less extensive. Now all regimes, regardless of political complexion, can aspire to total surveillance of *electronic* communications which are deployed by virtually everyone in all but the poorest societies. But the associated power relationships are different in key respects: first, the providers of the communications infrastructure are overwhelmingly in the private sector and this surveillance can take place only through complex webs of collaboration and collusion between state and corporate actors. Second, the very same communications revolution has given rise to unprecedented opportunities for resistance—or 'sousveillance'—by people challenging state or corporate power. But this is just as Janus-faced as surveillance itself – it may be deployed for progressive, democratic and emancipatory goals by insurgents against unjust rule but it may be used for predatory, exploitative or repressive ends by those trafficking in people, arms or drugs.

Only time will tell whether Edward Snowden has just shown a bit more of the intelligence body which contributes to enhanced understanding among the public or whether his actions have left the agencies shivering naked in the cold. Either way, we can no more disinvent technological surveillance mechanisms than abolish sin, so the political task is to seek legal and political structures for control and oversight that maximise the positive and minimise the negative uses of communications surveillance. This, whether we like it or not, requires the use of state structures. The minimum that is required for oversight of contemporary intelligence activities is a professional, full-time corps of lawyers, technologists and investigators, which would report to Parliament, and thereby the public, as to whether or not the infringements of privacy necessitated by communications surveillance are legitimate.

States may only be able to carry out their security roles through increased integration with private power but they alone may respond to democratic pressures. We must be alert to the permanent potential that states will abuse their power and damage the rights of citizens but, properly used, they are the only weapon we have against the irresponsible use of private power, whether it is in the form of a legal corporation or an illegal criminal organisation.

## Notes:

[1] Michael Hayden, former director both of NSA (1999-2005) and CIA (2006-2009) argued in a speech in London in September 2013 that US and UK agencies would have "to show a lot more leg" if they wanted to win broad public understanding and support for the kind of surveillance programmes they were undertaking. Cf. David Omand, "It's the most catastrophic loss to British intelligence ever, much worse than Burgess and Maclean in the 1950s," *BBC News*, 11 October 2013, http://www.bbc.co.uk/news/uk-24486649. This article takes events up to October 17, 2013.

[2] The NSA files published in the UK since 6 June 2013 by *Guardian* can be found at www.guardian.co.uk/world/the-nsa-files?INTCMP=SRCH.

[3] Glenn Greenwald, et al., "The Whisteblower," *Guardian*, 10 June 2013, 1-2.

[4] Paul Lewis and Spencer Ackerman, "Obama orders review of mass surveillance," *Guardian*, 10 August 2013, 1-2.

[5] See http://www.dnotice.org.uk.

[6] Cf. Simon Jenkins, "Snowden has started a global debate. Everywhere but here," *Guardian*, 20 September 2013, p. 35. But on October 11, the Deputy Prime Minister was reported as conceding the need for UK to update the system for legislative and political oversight. Patrick Wintour, et al., "Spies to go under spotlight," *Guardian*, 11 October 2013, p. 1.

[7] Richard Aldrich, *GCHQ: The Uncensored History of Britain's Most Secret Intelligence Agency* (London: Harper Press, 2010).

[8] Cf. Daveed Gartenstein-Ross and Kelsey D. Atherton, "How we killed privacy – in 4 easy steps," *Foreign Policy*, 23 August 2013, www.foreignpolicy.com/articles/2013/08/23/how_we_killed_privacy_nsa_surveillance.

[9] During his trial for a property offence, Malone discovered that police had been tapping his telephone. He challenged the legality of this but the UK court determined that there was no right to privacy in UK law. Accordingly, the Strasbourg court found that the procedures for authorisation of telephone tapping in UK, involving ministers but with no oversight or remedies for citizens, contravened Article 8 of the ECHR.

[10] There is a more extended discussion of the changing perception of risk at this time and its implications for intelligence in articles by Michael Warner, David Strachan-Morris, Mark Phythian and Peter Gill in *Intelligence and National Security* 27:2 (2012).

[11] Jessica Stern and Jonathan Wiener, "Precaution against terrorism," in Paul Bracken, Ian Bremmer, and David Gordon, eds., *Managing Strategic Surprise: Lessons from Risk Management and Risk Assessment* (Cambridge: Cambridge University Press, 2008), 110-83.

[12] Charles Cogan, "Hunters not gatherers: intelligence in the twenty-first century," *Intelligence and National Security* 19:2 (2004): 304-21.

[13] Matthew Aid, "The CIS's new black bag is digital," *Foreign Policy*, 17 July 2013.

[14] Jeffrey W. Seifert, *Data Mining: An Overview* (Washington, DC: Congressional Research Service, December 2004), p. 1, www.fas.org/irp (12 December 2011).

[15] But note this is always a silly metaphor, e.g. Mark Lowenthal, "The Real Intelligence Failure? Spineless Spies," *Washington Post*, 25 May 2008.

[16] Markle Foundation, *Creating a Trusted Information Network for Homeland Security,* Second Report of the Markle Foundation Task Force, December 2003, http://www.markle.org/publications/666-creating-trusted-network-homeland-security (19 December 2011).

[17] National Research Council, *Protecting Individual Privacy in the Struggle against Terrorists*: *A Framework for Program Assessment* (Washington, DC: National Academies Press, 2008).

[18] This may sound suspiciously like Rumsfeld's much derided discussion of 'known unknowns' and 'unknown unknowns,' but, actually, that distinction was one of the more sensible things uttered by the former US Defense Secretary.

[19] RIPA s.8 (1) warrants identify targeted people or places.

[20] E.g. Review Committee on the Intelligence and Security Services, "On the use of Sigint by DISS," *Annual Report* 2011-12, 37-110, quote on p. 81. John Lanchester reported that his reading of the Snowden files including this note on a presentation: "GCHQ policy is to treat it pretty much all the same whether it's content or metadata." See "Inside the Files: when did we give our consent to a secret state?" *Guardian*, 4 October 2013, 37.

[21] Patrick Radden Keefe, *Chatter* (New York, NY: Random House, 2006).

[22] Emphasis added by the author.

[23] Laurence Lustgarten and Ian Leigh, *In From the Cold: National Security and Parliamentary Democracy* (Oxford: Clarendon, 1994), 65-67.

[24] RCISS, 2011-12, 93-95.

[25] Cf. Victoria Williams, 2006, 74-75.

[26] Davis Omand, "Edward Snowden's leaks are misguided – they risk exposing us to cyber-attacks," *Guardian*, 26 September 2013. A fortnight later Omand was even more condemnatory, see note # 1.

[27] Nick Hopkins and Julian Borger, "Inside GCHQ: how US pays Britain's spy agency £100m for a very special relationship," *Guardian*, 2 August 2013, 1-2. Another example of US/UK legal distinctions came when *The Guardian*, under threat of legal injunction, allowed two GCHQ officials to oversee the destruction of hard drives containing Snowden's material at the paper's London office. US officials granted it was 'difficult to imagine' such a scenario in the US while the paper defended its actions on the grounds that other copies of the material existed in Brazil and the US and an injunction would have prevented its continued reporting. Julian Borger, "Secrets and threats – why hard drives were smashed," *Guardian*, 21 August 2013, pp. 4-5.

[28] Ed Pilkington, "Washington Post releases four new slides from NSA's Prism presentation," www.guardian.co.uk, 30 June 2013.

[29] Craig Timberg and Ellen Nakashima, "Agreement with private companies protect US access to cables' data for surveillance," *Washington Post*, 7 July 2013.

[30] James Bamford, "They know much more than you think," *The New York Review of Books*, 15 August 2013.

[31] James Bamford, "The NSA is Building the Country's Biggest Spy Center (Watch What You Say)," http://www.wired.com/threatlevel, 15 March 2012 (7 July 2013).

[32] www.guardian.co.uk/world/the-nsa-files?INTCMP=SRCH, see articles dated 21 June 2013.

[33] Glenn Greenwald, "How NSA can see 'nearly everything you do online'," *Guardian*, 1 August 2013, p. 1-2.

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

[35] Williams, 2006, 195-203.

[36] E.g. Dominic Rushe, "Yahoo and Microsoft express alarm over NSA attacks on online security," *Guardian*, 7 September 2013, p. 2.

[37] Bamford, 15 March 2012.

[38] James Ball, Julian Borger, and Glenn Greenwald, "Exclusive: how US and Britain unlock privacy on the internet," *Guardian*, 6 September 2013, pp. 1, 4-5.

[39] James Ball, et al., "NSA's attempt to crack web privacy tool used by dissidents is revealed," *Guardian*, 5 October 2013, 2. Some small CSPs based in US closed down their e-mail servers in order to protect customers' privacy: SominiSengupta, "2 e-mail services close and destroy data rather than reveal files," *New York Times*, 8 August 2013.

[40] E.g. Scott Shane and Nicole Perlroth, "Legislation seeks to bar NSA tactic in encryption," *New York Times*, 6 September 2013; Charles Arthur, "Academics criticise spy agencies," *Guardian*, 17 September 2013.

[41] Spencer Ackerman, "Senate interrogates NSA over extent of its snooping," *Guardian*, 13 June 2013, p. 24; Charlie Savage, "NSA Chief says surveillance has stopped dozens of plots," *New York Times*, 18 June 2013.

[42] E.g. Kenneth Roth, "Rethinking Surveillance," www.hrw.org, 2 July 2013. See also Charlie Savage and David Sanger, "Senate Panel presses NSA on phone logs," *New York Times*, 31 July 2013.

[43] David Sanger, "Budget documents detail extent of U.S. cyberoperations," *New York Times*, 31 August 2013.

[44] Dana Priest and William M. Arkin, "'Top Secret America': a look at the military's JSOC," *Washington Post*, 2 September 2011.

[45] Davis Omand, "Edward Snowden's leaks are misguided – they risk exposing us to cyber-attacks," *Guardian*, 26 September 2013.

[46] Eric Schmitt and Michael Schmidt, "Qaeda Plot has undermined U.S. intelligence," *New York Times*, 29 September 2013.

[47] Director of Security Service on MI5 and the Evolving Threat, 8 October 2013, www.rusi.org/events/past/ref:E5254359BB8F44.

[48] Julian Borger and Ian Traynor, "Brazilian president launches ferocious attack on NSA spying," *Guardian*, 25 September 2013, p. 4.

[49] Jonathan Weisman, "Momentum builds against NSA surveillance," *New York Times*, 28 July 2013; Spencer Ackerman and Paul Lewis, "In Snowden's wake, Congress cools on spying," *Guardian*, 3 August 2013.

[50] Paul Lewis and Dan Roberts, "Senators join forces to rein in NSA spying," *Guardian*, 26 September 2013, p. 22.

[51] Paddy Ashdown, "Who watches the watchers?" *Guardian*, 13 June 2013, p. 13.

[52] James Ball, "Vodafone and BT pursued over role in GCHQ internet monitoring," *Guardian*, 9 August 2013, p. 5; Matthew Taylor and Nick Hopkins, "Campaigners take surveillance fight with GCHQ to European court," *Guardian*, 4 October 2013, p. 6.

[53] Spencer Ackerman, "NSA guideline breaches contradict assurances from the White house," *Guardian*, 17 August 2013, p. 20.

[54] *BBC News*, 22 August 2013.

[55] The issue of democratic control is discussed more fully in Peter Gill and Mark Phythian, *Intelligence in an Insecure World* (Cambridge: Polity, 2012), Chapter 8.

[56] Nick Hopkins, "Spy agencies "need to show more leg" says ex-NSA chief," *Guardian*, 1 October 2013, p. 2.

[57] Cited in *Guardian*, 22 August 2013, p. 6. Hague and Malcolm Rifkind, Chair of the ISC, are described as the "useful idiots of the security classes" by Simon Jenkins, 20 September 2013, op cit. In his reply, Rifkind seeks to reassure that "the British public is well aware that its intelligence agencies have neither the time nor the remotest interest in the emails or telephone conversations of well over 99% of the population who are neither potential terrorists nor serious criminals." "Intelligent Oversight," *Guardian*, 21 September 2013, p. 13.

[58] http://isc.independent.gov.uk is the ISC's web-site where copies of its reports can be found.

[59] For example, Peter Gill, "Evaluating Intelligence Oversight Committees: the UK Intelligence and Security Committee and the 'War on Terror'," *Intelligence and National Security* 22:1 (2007): 14-37; Anthony Glees, et al., *The Open Side of Secrecy: Britain's Intelligence and Security Committee* (London: The Social Affairs Unit, 2006); Mark Phythian, "The British Experience with Intelligence Accountability," *Intelligence and National Security* 22:1 (2007): 75-99.

[60] Rifkind, 21 September 2013, op cit.

[61] 2012 Annual Report of the ICC, HC571, 13 July 2013, esp. pp. 11-16.

[62] A Statement of the Chairman of the Intelligence and Security Committee of Parliament, http://isc.independent.gov.uk/news-archive/17july2013.

**About the author**

PETER GILL is Honorary Senior Research Fellow at the University of Liverpool, UK; previously Research Professor in Intelligence Studies at the University of Salford. He is the author of *Policing Politics* (London: Cass, 1994) and *Rounding Up the Usual Suspects?* (Aldershot: Ashgate, 2000) and co-author of *Intelligence in an Insecure World* (Cambridge: Polity, 2nd edition 2012). He is co-editor of the *PSI Handbook of Global Security and Intelligence: National Approaches*, 2 volumes (Westport: Praeger, 2008) and *Intelligence Theory: Key Questions and Debates* (London: Routledge, 2009). His current research is into the democratisation of intelligence in former authoritarian regimes, for which he was awarded a Leverhulme Emeritus Fellowship in 2010. *E-mail:* PGill1@liverpool.ac.uk.

## Bibliography

"2 e-mail services close and destroy data rather than reveal files." *New York Times* (2013).

Ackerman, Spencer, and Paul Lewis. "In Snowden's wake, Congress cools on spying." *Guardian* (2013).

Ackerman, Spencer. "NSA guideline breaches contradict assurances from the White house." *Guardian* (2013): 20.

Ackerman, Spencer. "Senate interrogates NSA over extent of its snooping." *Guardian* (2013): 24.

Aid, Matthew. "The CIS's new black bag is digital." *Foreign Policy* (2013).

Aldrich, Richard. *GCHQ: The Uncensored History of Britain's Most Secret Intelligence Agency*. London: Harper Press, 2010.

*Annual Report of the ICC*., 2012.

Arthur, Charles. "Academics criticise spy agencies." *Guardian* (2013).

Ashdown, Paddy. "Who watches the watchers?" *Guardian* (2013): 13.

Ball, James, Julian Borger, and Glenn Greenwald. "Exclusive: how US and Britain unlock privacy on the internet." *Guardian* (2013): 1, 4-5.

Ball, James. "NSA's attempt to crack web privacy tool used by dissidents is revealed." *Guardian* (2013): 2.

Ball, James. "Vodafone and BT pursued over role in GCHQ internet monitoring." *Guardian* (2013): 5.

Bamford, James. *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*. Wired.com, 2012.

Bamford, James. *They know much more than you think*. The New York Review of Books, 2013.

Borger, Julian, and Ian Traynor. "Brazilian president launches ferocious attack on NSA spying." *Guardian* (2013): 4.

Borger, Julian. "Secrets and threats – why hard drives were smashed." *Guardian* (2013): 4-5.

Cogan, Charles. "Hunters not gatherers: intelligence in the twenty-first century." *Intelligence and National Security* 19, no. 2 (2004): 304-21.

*Creating a Trusted Information Network for Homeland Security*. Markle Foundation Task Force, 2011.

## Bibliography

"2 e-mail services close and destroy data rather than reveal files." *New York Times* (2013).

Ackerman, Spencer, and Paul Lewis. "In Snowden's wake, Congress cools on spying." *Guardian* (2013).

Ackerman, Spencer. "NSA guideline breaches contradict assurances from the White house." *Guardian* (2013): 20.

Ackerman, Spencer. "Senate interrogates NSA over extent of its snooping." *Guardian* (2013): 24.

Aid, Matthew. "The CIS's new black bag is digital." *Foreign Policy* (2013).

Aldrich, Richard. *GCHQ: The Uncensored History of Britain's Most Secret Intelligence Agency*. London: Harper Press, 2010.

*Annual Report of the ICC*., 2012.

Arthur, Charles. "Academics criticise spy agencies." *Guardian* (2013).

Ashdown, Paddy. "Who watches the watchers?" *Guardian* (2013): 13.

Ball, James, Julian Borger, and Glenn Greenwald. "Exclusive: how US and Britain unlock privacy on the internet." *Guardian* (2013): 1, 4-5.

Ball, James. "NSA's attempt to crack web privacy tool used by dissidents is revealed." *Guardian* (2013): 2.

Ball, James. "Vodafone and BT pursued over role in GCHQ internet monitoring." *Guardian* (2013): 5.

Bamford, James. *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*. Wired.com, 2012.

Bamford, James. *They know much more than you think*. The New York Review of Books, 2013.

Borger, Julian, and Ian Traynor. "Brazilian president launches ferocious attack on NSA spying." *Guardian* (2013): 4.

Borger, Julian. "Secrets and threats – why hard drives were smashed." *Guardian* (2013): 4-5.

Cogan, Charles. "Hunters not gatherers: intelligence in the twenty-first century." *Intelligence and National Security* 19, no. 2 (2004): 304-21.

*Creating a Trusted Information Network for Homeland Security*. Markle Foundation Task Force, 2011.

Gartenstein-Ross, Daveed, and Kelsey D. Atherton. "How we killed privacy – in 4 easy steps." *Foreign Policy* (2013).

Gill, Peter, and Mark Phythian. *Intelligence in an Insecure World*. Cambridge: Polity, 2012.

Gill, Peter. "Evaluating Intelligence Oversight Committees: the UK Intelligence and Security Committee and the 'War on Terror'." *Intelligence and National Security* 22, no. 1 (2007): 14-37.

Glees, Anthony. *The Open Side of Secrecy: Britain's Intelligence and Security Committee*. London: The Social Affairs Unit, 2006.

Greenwald, Glenn. "How NSA can see 'nearly everything you do online'." *Guardian* (2013): 1-2.

Greenwald, Glenn. "The Whisteblower." *Guardian* (2013): 1-2.

Hopkins, Nick, and Julian Borger. "Inside GCHQ: how US pays Britain's spy agency £100m for a very special relationship." *Guardian* (2013): 1-2.

Hopkins, Nick. "Spy agencies "need to show more leg" says ex-NSA chief." *Guardian* (2013): 2.

"Inside the Files: when did we give our consent to a secret state?" *Guardian* (2013): 37.

"Intelligent Oversight." *Guardian* (2013): 13.

Jenkins, Simon. "Snowden has started a global debate. Everywhere but here." *Guardian* (2013): 35.

Keefe, Patrick Radden. *Chatter*. New York, NY: Random House, 2006.

Lewis, Paul, and Dan Roberts. "Senators join forces to rein in NSA spying." *Guardian* (2013): 22.

Lewis, Paul, and Spencer Ackerman. "Obama orders review of mass surveillance." *Guardian* (2013): 1-2.

Lowenthal, Mark. "The Real Intelligence Failure? Spineless Spies." *Washington Post* (2008).

Lustgarten, L, and I Leigh. *In From the Cold: National Security and Parliamentary Democracy*. Oxford: Oxford University Press, 1994.

Omand, David. *Snowden leaks 'worst ever loss to British intelligence'*. BBC News, 2013.

Omand, Davis. "Edward Snowden's leaks are misguided – they risk exposing us to cyber-attacks." *Guardian* (2013).

*On the use of Sigint by DISS* In *Annual Report* . Committee on the Intelligence and Security Services, 2011.

Phythian, Mark. "The British Experience with Intelligence Accountability." *Intelligence and National Security* 22, no. 1 (2007): 75-99.

Pilkington, Ed. *Washington Post releases four new slides from NSA's Prism presentation*., 2013.

Priest, Dana, and William M. Arkin. "'Top Secret America': a look at the military's JSOC." *Washington Post* (2011).

*Protecting Individual Privacy in the Struggle against Terrorists: A Framework for Program Assessment*. Washington, DC: National Academies Press, National Research Council, 2008.

Roth, Kenneth. *Rethinking Surveillance*., 2013.

Rushe, Dominic. "Yahoo and Microsoft express alarm over NSA attacks on online security." *Guardian* (2013): 2.

Sanger, David. "Budget documents detail extent of U.S. cyberoperations." *New York Times* (2013).

Savage, Charlie, and David Sanger. "Senate Panel presses NSA on phone logs." *New York Times* (2013).

Savage, Charlie. "NSA Chief says surveillance has stopped dozens of plots." *New York Times* (2013).

Schmitt, Eric, and Michael Schmidt. "Qaeda Plot has undermined U.S. intelligence." *New York Times* (2013).

Seifert, Jeffrey W.. *Data Mining: An Overview*. Washington, DC: Congressional Research Service, 2004.

Shane, Scott, and Nicole Perlroth. "Legislation seeks to bar NSA tactic in encryption." *New York Times* (2013).

Stern, Jessica, and Jonathan Wiener. "*Precaution against terrorism*." In *Managing Strategic Surprise: Lessons from Risk Management and Risk Assessment*, 110-83. Cambridge: Cambridge University Press, 2008.

Taylor, Matthew, and Nick Hopkins. "Campaigners take surveillance fight with GCHQ to European court." *Guardian* (2013): 6.

Timberg, Craig, and Ellen Nakashima. "Agreement with private companies protect US access to cables' data for surveillance." *Washington Post* (2013).

Warner, Michael, David Strachan-Morris, Mark Phythian, and Peter Gill. "Discussion of the changing perception of risk at this time and its implications for intelligence in articles ." *Intelligence and National Security* 27, no. 2 (2012).

Weisman, Jonathan. "Momentum builds against NSA surveillance." *New York Times* (2013).

Wintour, Patrick. "Spies to go under spotlight." *Guardian* (2013): 1.

Gartenstein-Ross, Daveed, and Kelsey D. Atherton. "How we killed privacy – in 4 easy steps." *Foreign Policy* (2013).

Gill, Peter, and Mark Phythian. *Intelligence in an Insecure World*. Cambridge: Polity, 2012.

Gill, Peter. "Evaluating Intelligence Oversight Committees: the UK Intelligence and Security Committee and the 'War on Terror'." *Intelligence and National Security* 22, no. 1 (2007): 14-37.

Glees, Anthony. *The Open Side of Secrecy: Britain's Intelligence and Security Committee*. London: The Social Affairs Unit, 2006.

Greenwald, Glenn. "How NSA can see 'nearly everything you do online'." *Guardian* (2013): 1-2.

Greenwald, Glenn. "The Whisteblower." *Guardian* (2013): 1-2.

Hopkins, Nick, and Julian Borger. "Inside GCHQ: how US pays Britain's spy agency £100m for a very special relationship." *Guardian* (2013): 1-2.

Hopkins, Nick. "Spy agencies "need to show more leg" says ex-NSA chief." *Guardian* (2013): 2.

"Inside the Files: when did we give our consent to a secret state?" *Guardian* (2013): 37.

"Intelligent Oversight." *Guardian* (2013): 13.

Jenkins, Simon. "Snowden has started a global debate. Everywhere but here." *Guardian* (2013): 35.

Keefe, Patrick Radden. *Chatter*. New York, NY: Random House, 2006.

Lewis, Paul, and Dan Roberts. "Senators join forces to rein in NSA spying." *Guardian* (2013): 22.

Lewis, Paul, and Spencer Ackerman. "Obama orders review of mass surveillance." *Guardian* (2013): 1-2.

Lowenthal, Mark. "The Real Intelligence Failure? Spineless Spies." *Washington Post* (2008).

Lustgarten, L, and I Leigh. *In From the Cold: National Security and Parliamentary Democracy*. Oxford: Oxford University Press, 1994.

Omand, David. *Snowden leaks 'worst ever loss to British intelligence'*. BBC News, 2013.

Omand, Davis. "Edward Snowden's leaks are misguided – they risk exposing us to cyber-attacks." *Guardian* (2013).

*On the use of Sigint by DISS* In *Annual Report* . Committee on the Intelligence and Security Services, 2011.

Phythian, Mark. "The British Experience with Intelligence Accountability." *Intelligence and National Security* 22, no. 1 (2007): 75-99.

Pilkington, Ed. *Washington Post releases four new slides from NSA's Prism presentation*., 2013.

Priest, Dana, and William M. Arkin. "'Top Secret America': a look at the military's JSOC." *Washington Post* (2011).

*Protecting Individual Privacy in the Struggle against Terrorists: A Framework for Program Assessment*. Washington, DC: National Academies Press, National Research Council, 2008.

Roth, Kenneth. *Rethinking Surveillance*., 2013.

Rushe, Dominic. "Yahoo and Microsoft express alarm over NSA attacks on online security." *Guardian* (2013): 2.

Sanger, David. "Budget documents detail extent of U.S. cyberoperations." *New York Times* (2013).

Savage, Charlie, and David Sanger. "Senate Panel presses NSA on phone logs." *New York Times* (2013).

Savage, Charlie. "NSA Chief says surveillance has stopped dozens of plots." *New York Times* (2013).

Schmitt, Eric, and Michael Schmidt. "Qaeda Plot has undermined U.S. intelligence." *New York Times* (2013).

Seifert, Jeffrey W.. *Data Mining: An Overview*. Washington, DC: Congressional Research Service, 2004.

Shane, Scott, and Nicole Perlroth. "Legislation seeks to bar NSA tactic in encryption." *New York Times* (2013).

Stern, Jessica, and Jonathan Wiener. "*Precaution against terrorism*." In *Managing Strategic Surprise: Lessons from Risk Management and Risk Assessment*, 110-83. Cambridge: Cambridge University Press, 2008.

Taylor, Matthew, and Nick Hopkins. "Campaigners take surveillance fight with GCHQ to European court." *Guardian* (2013): 6.

Timberg, Craig, and Ellen Nakashima. "Agreement with private companies protect US access to cables' data for surveillance." *Washington Post* (2013).

Warner, Michael, David Strachan-Morris, Mark Phythian, and Peter Gill. "Discussion of the changing perception of risk at this time and its implications for intelligence in articles ." *Intelligence and National Security* 27, no. 2 (2012).

Weisman, Jonathan. "Momentum builds against NSA surveillance." *New York Times* (2013).

Wintour, Patrick. "Spies to go under spotlight." *Guardian* (2013): 1.