This is an Accepted Manuscript of a book chapter published by Routledge in TERRORISM AND STATE SURVEILLANCE OF COMMUNICATIONS on 30 May 2019, available online: https://www.routledge.com/Terrorism-and-State-Surveillance-of-Communications-1st-Edition/Hale-Ross-Lowe/p/book/9780367025403

2 Intelligence gathering, issues of accountability, and Snowden

Julian Richards

Introduction

The first years of the twenty-first century saw a nexus of two issues that led, eventually, to the recasting of interception law in many Western states. The first of these was a growing awareness in the security agencies that communications technology and behaviours were changing in such a fundamental way that traditional approaches to achieving signals interception (SIGINT) were coming under serious question. Then. in May 2013, a contractor working for the US government by the name of Edward Snowden broke ranks and facilitated the publication of a welter of highly classified documents concerning the SIGINT activities of the US National Security Agency (NSA) and those of its key partners, notably Britain's Government Communications Headquarters (GCHQ). These exposed an industrial-scale process of bulk communications interception at a scale that most could not have imagined. It also posed serious questions about whether and how Western oversight bodies had known about these activities and been part of any debate about them.

AU: I have made signals interception all lower case and its acronym upper case. Please confirm if this is okay. Please confirm if the definition should be 'signals interception' or 'signals intelligence'.

These developments brought together two sets of public debates that pivoted around the perennial question of privacy versus security. Whether or not Snowden was right to reveal the extent of information that he revealed, he certainly did ignite a debate across Western countries about the acceptable levels of modern-day interception activity and how European states should interact with their American partners.

In the UK, Snowden's revelations had the effect of punctuating a debate already underway about whether and how surveillance and interception law should be changed to reflect the new technological – and perhaps ethical – environment. The debates led in time to the drafting of a new Bill, called the Investigatory Powers Act (IPA), which eventually passed into law at the end of 2016 after very extensive debate and scrutiny, including a challenge from the Court of Justice of the European Union (CJEU).

We could ask the question as to whether Snowden's actions, which place him in exile in Russia facing multiple years in jail should he return to the US, caused a retrenchment of industrial-scale Western surveillance and interception activities. The answer, perhaps ironically, is that the opposite seems to have happened. Taking the UK's IPA as an example, many Western states continue to have considerable interception capabilities and powers and have arguably deepened and strengthened these powers in many cases. Indeed, it could be argued that the state's professed need to continue to be able to tackle the security threats of the twenty-first century despite significant changes in technology have won out over any public concerns that may exist about erosions of privacy. As a side issue, continuing questions about whether Western oversight and accountability regimes have sufficient teeth to be able to take on the security agencies seem only to have been exacerbated.

This chapter will consider the chronology of events in the UK case study, starting in the late 2000s and moving on to the passing of the IPA in 2016. It interprets this story in terms of whether and how the state interacted with its critics in developing a refreshed surveillance regime; how the oversight bodies fared throughout the period; and where this leaves questions of privacy-versus-security in the final analysis.

Snowden's revelations

In late May 2013, a contractor working for the US firm Booz Allen Hamilton by the name of Edward Snowden, travelled from Hawaii to Hong Kong. He was carrying a set of laptops on which were stored approximately 1.7 million classified documents that he had extracted from the National Security Agency (NSA's) databases. Once in Hong Kong, he met with two journalists and a documentary film-maker, and on 5 June 2013, *The Guardian* newspaper in the UK published the first of a set of hitherto highly classified revelations derived from these documents. The details implicated not only the NSA but also its key SIGINT partner, GCHQ, in industrial-scale interception and collection of global communications at a scale and method that were, so it was implied, hugely disproportionate and potentially unlawful. On 9 June, Snowden went public himself for the first time with an interview aired on the internet in which he claimed that 'he had done nothing wrong'.[1] On 23 June, having been stripped of his passport other than for the purpose of returning to the US, he was allowed entry to Moscow.

AU: I have added the year to clarify the timeline. Please verify the change.

1 Mirren Gidda (2013) 'Edward Snowden and the NSA files – timeline', *The Guardian*, 21 August 2013, retrieved from www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline [accessed 4 April 2018].

The impact of the revelations on intelligence operations in the US, UK, and elsewhere is virtually impossible to delineate from the outside. A recent head of MI5 has been quoted as saying the disclosure of the details was a 'gift' to terrorists,[2] as they could tighten-up their communications security now that they had a better knowledge of how the major intelligence services attempted to monitor them. The US's Director of National Intelligence at the time, James Clapper, told the Senate Intelligence Committee that Snowden's revelations had caused 'grave damage' to the intelligence operation.[3] Meanwhile, the former chief of both NSA and CIA, General Michael Hayden, found himself in hot water shortly after the revelations by responding to a question on whether Snowden should be on the list of nominees for the European Parliament's Sakharov Prize for Freedom of Thought, by admitting he had briefly pondered whether there was a different list that might have more appropriately borne Snowden's name.[4] Whatever the difficulties, it seems likely that the sheer scale of the leaked documentation and the very high levels of classification that had previously applied to much of it, suggest that potentially considerable risk was generated for the protection of sensitive capabilities and their effective operation following Snowden's disclosures.

In civil society, meanwhile, the questions were not so much about the potential damage caused to the intelligence operation by the disclosures, or indeed about the illegality or moral purpose of the way in which Snowden had stolen and leaked the documents, although these were subjects of sometimes heated discussion. Instead, the key questions were about both the spirit and letter of the law when considering the way in which major intelligence agencies on both sides of the Atlantic were operating. Much of this debate found itself in the philosophically grey area of the appropriate balance between privacy and security in the modern age, and where the line should be drawn to indicate appropriate levels of national security policy. The civil society perspective has also highlighted the question of whistle-blowers and whether and how they should be protected in democratic states. While many in the intelligence business felt that Snowden was a traitor and a criminal, many in the realm of civil liberties activism felt that he was a heroic figure. Indeed, one of Snowden's first visitors

2 Cited in Michael V. Hayden (2014) 'Beyond Snowden: An NSA reality check', *World Affairs*, 176(5), 13–23.

3 Cited in Dave Weinstein (2014) 'Snowden and US cyber power', *Georgetown Journal of International Affairs*, 4, 4–11.

4 Michael V. Hayden (2014) 'Beyond Snowden: An NSA reality check', *World Affairs*, 176(5), 13–23.

in Moscow on his arrival was Jesselyn Radack, the US-based civil rights lawyer, who travelled to the Russian capital to present Snowden with an 'Integrity in Intelligence' award.[5]

Questions of technology

General Hayden is right to claim that concerns about large-scale SIGINT exploitation by the major national security states did not come out of a clear blue sky with Snowden's revelations in June 2013.[6] In large part, the debate was already underway and being driven by the two not entirely complementary pressures of changes in technology that were making traditional approaches to SIGINT more difficult, and there was also a massive explosion of personal data in cyberspace that raised extremely complex and ambiguous questions about the rights to, and boundaries of, privacy.

AU: I have changed 'twin' to 'two'. Please verify if the change is acceptable.

In the UK, a year before Snowden's disclosures, the government had invited the parliamentary Intelligence and Security Committee (ISC) to launch an inquiry that would feed into pre-legislative scrutiny of a new Bill governing the question of access by the security agencies to communications data (that is, data about communications events rather than their content). The issue had been simmering for some time, since it was increasingly being recognised that changes in communications network configurations and in communications behaviours were leading to a gradual dwindling in the amount of traditional communications data the police and intelligence services could access to support their investigations. In particular, the rise of bundled contracts for consumers in which communications events were charged not by individual events but within general tariffs meant that the communications service providers (CSPs) were increasingly dropping plans to keep the sort of data traditionally characterised as 'billing records', since there was no commercial need to do so. The problem for the security agencies in the disappearance of these records (generally considered by them to be critical for analysing networks of individuals of interest) seemed to be compounded by the rise of internet-based communications, to which traditional notions of communications events and 'metadata' did not so easily apply. In their report on the draft Bill, published in February 2013, the ISC noted that the police, intelligence services, and selected other public bodies had made

AU: Semi colon after 'more difficult' changed to an independent clause for clarity.

5 Wikileaks, (2013) 'Video: Edward Snowden wins Sam Adams award Friday' (12 October 2013), retrieved from https://wikileaks.org/Video-Edward-Snowden-wins-Sam.html [accessed 12 August 2018].

6 Michael V. Hayden (2014) 'Beyond Snowden: An NSA reality check', *World Affairs*, 176(5), 13–23, p.14.

approximately 500,000 requests for communications data from CSPs in the preceding year and that such data were 'immensely valuable' to investigations into serious crime and terrorism.[7]

The road to the 2016 Investigatory Powers Act 2016

Thus were commenced deliberations about a new Bill initially called the Communications Data Bill, which in 2016 eventually evolved into the wider Investigatory Powers Act (IPA). The beginning of the journey towards the realisation of this new law, however, starts some time before Snowden's revelations. Indeed, it is appropriate to go back to the general election of 2010 to identify where the issue had started to become particularly problematic in the UK. In this election, a Conservative-Liberal Democrat coalition government was the eventual result of a failure to achieve an overall majority by any of the major parties.

On the question of the expansion or retrenchment of the state's surveillance capabilities, we might suppose that the two partners in the coalition fell generally on either side of the line. To some extent this was true, although not entirely so. It was certainly the case that the nature of the coalition was such that sufficient votes to pass a proposed new Bill on access to communications data in parliament could not be assured. Much of the Conservative Party, led by Prime Minister David Cameron and the then Home Secretary, Theresa May, were sufficiently convinced by the security services' ticking-clock narrative about the dangers of the aforementioned decline in the capability to exploit communications data. But the Deputy Prime Minister and leader of the Liberal Democrats, Nick Clegg, had decried the proposed new Bill as a 'snooper's charter'; that is, a blank cheque for the state to spy on the populace at will. Clegg positioned himself as something of a gatekeeper against the more surveillance-minded instincts of some of his Conservative Party colleagues, warning that the new Bill, 'won't happen while Lib Dems are in government'.[8]

In the UK, two processes followed the release of the Snowden files in 2013. The first and most pressing issue was a very specific allegation of illegality on GCHQ's part concerning a secret NSA operation called PRISM. This operation concerned the large-scale collection of communications data and content from US-based internet service providers (ISPs) under the mandate of the Foreign Intelligence Services Act (FISA), this is

7 Intelligence and Security Committee (2013) 'Access to communications data by the intelligence and security Agencies', report presented to Parliament, Cm 8514, February 2013, p.8.

8 Stewart Mitchell (2013) 'Lib Dems block "snooper's charter"' (25 April 2013), retrieved from www.alphr.com/politics/22986/lib-dems-block-snoopers-charter [accessed 19 August 2018].

an act passed in 1975 following the Church Committee inquiry that allows US security agencies to gain selective access to the communications of US-based individuals. (The act was initially aimed at the interception of the communications of hostile foreign intelligence personnel based in embassy premises in the US, but it can also be used on suspected terrorist targets using US-based CSPs.) Because the Snowden files revealed that GCHQ had also had extensive access to such FISA-authorised data through PRISM since 2007, allegations started to circulate in the UK press that the British agency was effectively gaining unwarranted access to the communications of UK individuals through their American partner.[9] Following scrutiny of GCHQ files and processes, the ISC concluded robustly in July 2013 that no illegal access to such communications had taken place.[10]

However, the genie was now out of the bottle, and the ISC decided that a much broader investigation into the activities of GCHQ and other security agencies in the post-Snowden environment had become appropriate. This led to the Privacy and Security Inquiry which took evidence over many months from a wide range of security agency personnel (including the chiefs of the UK three intelligence agencies) and in addition, academics, technicians, journalists, and representatives of civil liberties organisations. The subsequent report, entitled 'Privacy and security: A modern and transparent framework' was published nearly two years later in March 2015.

Before the final report was published, however, the government initiated a series of events which constituted a cycle between legislation and challenge in the courts, with the CJEU playing a key role.

By 2014, the government found itself facing three problems concerning continued access to communications data. The first was the technology problem described above, which many inside the security agencies felt was reaching crisis point. The second was the lack of political consensus on the issue within the coalition government, in which the Liberal Democrats had expressly said they would oppose the new Communications Data Bill. To these two challenges was added a judgement by the CJEU which suggested that the UK's current practice in this area, as defined by the 2000 Regulatory and Investigatory Powers Act (RIPA), was incompatible with the 2009 Data Retention Directive. Specifically, two areas of concern were highlighted: That internal authorisation for communications data requests in the UK did not involve sufficient scrutiny and that requests were not being restricted to matters concerning serious crime (including terrorism).

9 Intelligence and Security Committee (2013) 'Statement on GCHQ's alleged interception of communications under the US PRISM programme' (July 2013), retrieved from http://isc.independent.gov.uk/committee-reports/special-reports [accessed 20 September 2018].

10 Ibid.

This, it was suggested, meant that UK law was not providing sufficient protection of privacy under the 1998 Human Rights Act.

In response, the government took the controversial step of introducing an emergency piece of legislation called the Data Retention and Investigatory Powers Act (DRIPA), announced in parliament by the then Home Secretary Theresa May on 10 July 2014.[11] The aim of this legislation was to ensure that the security agencies could continue to gain access to communications data from CSPs. Indeed, it introduced a new legal mandate for relevant companies to retain such data for a year and make it available to the government as requested – while allowing debate and discussion to continue in the background. This would culminate in a new, over-arching law. A year later, the Conservative Party established an overall majority in the general election and was able to form a government without the Liberal Democrats, thus removing one of their obstacles to legislating in this area.

DRIPA proved to be a hot political potato. Immediately following its introduction, two MPs from across the political divide joined forces with a group of civil liberties NGOs to take the government to court on the issue. The alliance of David Davis, a Conservative MP with strong civil libertarian sentiments, who would later become the government's first Brexit minister, and Tom Watson, who later became the deputy leader of the Labour Party, demonstrated the way in which the issue of state surveillance versus privacy rights cuts across traditional political fault lines. The two MPs joined forces with Liberty, Open Rights Group, Amnesty, and Privacy International to bring the case that DRIPA was incompatible with European human rights and data retention law. Just short of a year after Theresa May's announcement of DRIPA in Parliament, the High Court ruled against the government and upheld the charge that DRIPA was 'inconsistent with European Union Law'.[12]

The government appealed this decision, taking the case to the CJEU in Luxembourg, but before this appeal was heard, the ISC had reported the findings of its major Privacy and Security Inquiry. The report preceded by three months the publication of a second report, commissioned separately from the government's Independent Reviewer of Terrorism Legislation, David Anderson QC, and published under the title 'A question of trust'.[13] Both reports informed

11 Home Office (2014) 'Home Secretary's oral statement about the use of communications data and interception' (10 July 2014), retrieved from www.gov.uk/government/speeches/communications-data-and-interception [accessed 25 September 2018].

12 Owen Bowcott (2015) 'High Court rules data retention and surveillance legislation unlawful', *The Guardian*, 17 July 2015, retrieved from www.theguardian.com/world/2015/jul/17/data-retention-and-surveillance-legislation-ruled-unlawful [accessed 5 April 2018].

13 David Anderson QC (2015) 'A question of trust – report of the investigatory powers review', 11 June 2015, retrieved from www.daqc.co.uk/2015/06/11/a-question-of-trust-report-of-the-investigatory-powers-review/ [accessed 5 August 2018].

the drafting of the new IPA Bill that commenced pre-legislative scrutiny in March 2016 and received Royal Assent in November of that year.

One of the key elements of the ISC's 'Privacy and security' report, concerned legislation governing investigatory activities, and specifically the notion that RIPA and related pieces of legislation were too complex for anyone to easily navigate through, and were ill-equipped for affording privacy protections in the modern age of communications. The government's loss of the case in the High Court had further heightened anxieties. The key recommendation in the ISC report was therefore that, 'the current legal framework be replaced by a new Act of Parliament governing the intelligence and security Agencies'[14] and was duly heeded with the drafting of the new Bill. The ISC did stress that its investigations into the work of the intelligence agencies gave it no cause to consider that the Human Rights Act was not being respected (a judgement at odds with the case brought by MPs Davis and Watson) but that the legal regime had become 'unnecessarily complicated' over the years. The Interception of Communications Commissioner, Sir Anthony May, was less charitable, noting in his 2013 annual report that[15] 'RIPA 2000 Part I Chapter I is difficult legislation and a reader's eyes glaze over before reaching the end of section 1, that is, if the reader ever starts'.

AU: 'A question of trust' changed to lowercase to match usage elsewhere.

Anderson's 'A question of trust' report came to similar conclusions, suggesting that a 'comprehensive and comprehensible new law should be drafted from scratch, replacing the multitude of current powers'.[16] Perhaps sharing Sir Anthony May's feelings, the Anderson report noted that:

> RIPA, obscure since its inception, has been patched up so many times as to make it incomprehensible to all but a tiny band of initiates. A multitude of alternative powers, some of them without statutory safeguards, confuse the picture further. This state of affairs is undemocratic, unnecessary and, in the long run, intolerable.[17]

14 Intelligence and Security Committee (2015) 'Privacy and security: A modern and transparent legal framework', report presented to Parliament, HC 1075 (12 March 2015) p.2.

15 Sir Anthony May (2014) '2013 Annual report of the Interception of Communications Commissioner', HC 1184 (8 April 2014), retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/302600/InterceptionCommunicationsCommissionerAccessible.pdf [accessed 5 April 2018] p.61.

16 David Anderson QC (2015) 'A question of trust – report of the Investigatory Powers Review', 11 June 2015, retrieved from www.daqc.co.uk/2015/06/11/a-question-of-trust-report-of-the-investigatory-powers-review/ [accessed 5 August 2018] p.4.

17 David Anderson QC (2015), 'A question of trust – report of the Investigatory Powers Review', 11 June 2015, retrieved from www.daqc.co.uk/2015/06/11/a-question-of-trust-report-of-the-investigatory-powers-review/ [accessed 5 August 2018] p.8.

David Anderson went further in suggesting that the three surveillance commissioners' offices should be combined into one new Independent Surveillance and Intelligence Commission (ISIC), and that crucially this office should oversee the activities of a new set of judicial commissioners who would provide a second layer (on top of ministerial authorisation) to the authorisation of interception warrant requests.[18]

Such a suggestion would mark a significant departure from, and strengthening of, intelligence authorisation processes, albeit in the more highly intrusive area of content interception rather than that of the gathering of communications data, which, to a large extent, remained subject to the same level of authorisation in the new Bill as had been the case before.

The new IPA Bill was duly drafted and scrutinised and passed into law in December 2016. It incorporated many (though not all) of the recommendations of the various processes and reports informing its development. Many of its elements were not greatly dissimilar from those mandated under the former RIPA law, while some were quite different, and notably the requirement for 'double-lock' authorisation for content access warrants to be signed by a minister and a judicial commissioner.

On the political scene, Theresa May had become Prime Minister following David Cameron's resignation in July 2016, but she managed to lose her parliamentary majority in the general election a year later, necessitating a new coalition with the Democratic Unionist Party (DUP) of Northern Ireland. While Brexit had become her government's primary focus, the question of surveillance law suffered a further complication in December 2017, when the CJEU finally completed its deliberations on the DRIPA appeal and upheld the judgement of the UK's High Court in ruling that the act was unlawful. Although DRIPA had since been superseded by the IPA, many of the former's elements had been incorporated into the latter, thus casting fresh doubt over the legality of the IPA under European law.[19] This remains an unresolved legislative conundrum at the time of writing.

Reactions to the new IPA

At the stage of pre-legislative scrutiny, the ISC offered a mixed response to the proposed new law. The chairman of the ISC, Dominic Grieve, noted with satisfaction that many of the recommendations in the 2015 'Privacy

18 David Anderson QC (2015) 'A question of trust – report of the Investigatory Powers Review', 11 June 2015, retrieved from www.daqc.co.uk/2015/06/11/a-question-of-trust-report-of-the-investigatory-powers-review/ [accessed 5 August 2018] p.7.

19 Alexander J Martin (2016) 'Landmark EU ruling: Legality of UK's Investigatory Powers Act challenged', *The Register*, 21 December 2016, retrieved from www.theregister.co.uk/2016/12/21/eu_judgment/ [accessed 5 April 2018].

and security' report, notably those concerning strengthening the explicit authorisation of bulk personal datasets, bulk communications data, and 'computer network exploitation' (for which we should read computer hacking) had been acted upon[20]. However, Grieve conveyed 'disappointment' that the IPA did not mark a comprehensive re-drafting and consolidation of all surveillance law, but merely those elements concerning the interception and exploitation of communications and related data and cyber activities. Thus, other activities, such as covert surveillance and human intelligence operations, for example, continue under the auspices of the old RIPA law. This was, in the view of Grieve, a 'missed opportunity', and it remained the case in his view that the new bill, 'fails to deliver the clarity that is so badly needed in this area'.[21]

Perhaps more seriously, the ISC chairman expressed disquiet about the clarity of privacy protections in the new law, suggesting that it had adopted a rather 'piecemeal' approach in which there was no universal definition of the approach to privacy.[22]

In this way, we could conclude that, rather than simplifying and clarifying the overall approach to surveillance that had been a perceived problem with the 'piecemeal' and 'obscure' set of laws previously in place, the ISC's conclusion is that the IPA has added to the confusion in some respects. As David Anderson noted above, this is not only tedious for those attempting to navigate through the law, but could even be perceived as fundamentally undermining of privacy protections in a modern democracy.

It is worth noting that the question of whether updating surveillance law improves or further complicates the situation, is not one confined to the UK. Other European countries, both before and after the Snowden revelations, have grappled with the same challenges in trying to balance updated capabilities with concerns over privacy. Notable cases have included a case brought by the civil rights group Digital Rights Ireland concerning the retention of communications data by the Irish police, and a challenge brought against the Swedish government over the privacy protections afforded by interception law. In Germany, Snowden's revelations led directly to the formation of an ad hoc cross-parliamentary inquiry, called the 'NSA inquiry' (*Untersuchungsausschuss*, NSA) launched in March 2014, prompted by concerns over the depth of the SIGINT relationship with the US. This inquiry uncovered concerns and weaknesses in the authorisation process for

20 Intelligence and Security Committee (2016) 'Press release' (9 February 2016) retrieved from http://isc.independent.gov.uk/news-archive?offset=10 [accessed 5 August 2018].

21 Ibid.

22 Ibid.

SIGINT collection by the *Bundesnachrichtendienst* (BND), particularly as regards bulk data collection against foreign nationals, including close EU partners. The outcome was a set of legislative changes governing the activities of the BND, which were completed by 2016. Wetzling's verdict on these changes is generally rather damning: not only did they, 'not fix the country's woefully inadequate judicial oversight system'[23] but introduced new confusions and gaps in the oversight machinery, leaving parliamentary oversight of intelligence 'fragmented'.[24]

Whether such developments mark a conscious attempt by European states to obfuscate the law around surveillance and make the lives of the overseers more difficult, seems doubtful. At the same time, Snowden himself noted that NSA had been working with their SIGINT partners in Germany, the Netherlands, and Sweden to consider how they could make their laws more conducive to SIGINT operations, citing the UK's GCHQ as the model. This does at least show that the SIGINT agencies are very aware of the laws governing their activities and will be thinking about how best to achieve what they want to achieve within the legislative framework.

In terms of how the new IPA came about, it could be interpreted, as David Anderson did, that intense parliamentary scrutiny was undertaken for a period approaching ten years before the new law was passed concerning interception activities. An early version of this, the Communications Data Bill, was rejected by Parliament and further drafting was undertaken. A major period of scrutiny by a joint committee across the two houses of Parliament, in addition to two major reports by the ISC and by the Independent Reviewer of Terrorism Legislation, were all brought to bear on the deliberations leading to the drafting of the new Bill, and some major changes to the authorisation and oversight regime governing interception were subsequently written in. While the DRIPA law was instituted as a piece of emergency legislation in 2014, it is fair to say that the over-arching process of reviewing and changing the law could hardly be criticised as being either rushed or not subject to extensive parliamentary scrutiny. In this way, one could argue, democracy appears to have been working entirely appropriately and effectively.

These are the arguments for the executive's position on the matter, but it is worth considering the concerns. It is fair to say that political changes

23 Thorsten Wetzling (2013) 'Germany's intelligence reform: More surveillance, modest restraints and inefficient controls', *Stiftung Neuer Verantwortung*, June 2017, retrieved from www.researchgate.net/publication/318393882_Germany's_intelligence_reform_More_surveillance_modest_restraints_and_inefficient_controls. p.3.

24 Ibid.

over the period in question worked in favour of the Conservative Party in that a situation during coalition government when it was proving impossible to pass a new interception law gradually fell away in tandem with support for the Liberal Democrats at the polls. Once the Conservatives had established their own majority government in 2015, progress towards the new Bill accelerated.

The recent CJEU's ruling on the unlawfulness of certain provisions of the DRIPA Bill pose extremely complicated questions for the IPA in those areas where DRIPA provisions were adopted. The suggestion is that the government has been allowing far too wide an application of intrusive surveillance powers, extending beyond serious crime and national security and into other areas of monitoring, such as tax and benefit compliance. Secondly, the pre-existing model of separating communications content exploitation from the exploitation of communications data in terms of their relative intrusiveness has been somewhat blown apart by the CJEU. In the former, the IPA has greatly strengthened the authorisation regime, requiring not only ministerial sign-off on content interception warrants but also secondary approval from one of the new judicial commissioners. For communications data, however, the former level of authorisation has been retained, namely a 'bulk access' authorisation such that individual requests for batches of data need only be signed off by an appointed manager within the security agency in question. Furthermore, the CSPs now have a legal obligation under the IPA to retain such data for up to a year, should they need to make it available to a requesting government body.

The CJEU upheld the High Court's ruling that the existing procedures do not provide adequate privacy protections to the public in the area of accessing communications data, and it is worth noting that such data now includes internet logging details as well as telephone call records. Restricting access amongst government departments to those dealing only with the most serious of cases may not be a huge problem, since the ISC noted in its February 2013 report (published before Snowden's revelations) that less than one percent of all communications data requests generally come from local authorities other than the main security agencies.[25] However, applying an extra layer of authorisation to all communications data requests would be a serious complication, given that the same ISC report observed there were approximately half a million such requests made every year. The government has proposed some changes to the IPA and taken the unusual step of

AU: Is there a date for the Cm to add to the foontnote?

25 Intelligence and Security Committee (2013) 'Access to communications data by the intelligence and security agencies', report presented to Parliament, Cm 851.

laying these proposals out for consultation,[26] although it is fair to say that the CJEU's ruling does pose some very difficult procedural questions.

In the meantime, an overall assessment of the IPA could conclude that it allows the government to recover ground against the very changes it was fearing at the beginning of the process. In essence, nothing has changed in terms of the state's continued capability in the area of interception. Indeed, on the question of access to communications data, the state has strengthened its hand by now being able to legally mandate the retention of and access to such data from the CSPs. Other activities that were underway before, such as cyber-operations ('computer network exploitation') continue, but with an added cloak of legal statute. If the government's objective was to be able to retain the capabilities it had in communications and computer exploitation in the face of rapid and substantial technological change, then it appears to have achieved this aim.

For many in the field of civil liberties, however, this is far from a great outcome, and means that the questions posed by Snowden about the reach of the most powerful national security states have not been adequately addressed. Jen Stout of the NGO, Civil Society Futures, claimed that the passing of the IPA in 2016, 'marked the point that the British government went off the deep end in terms of surveillance and authoritarianism'.[27] Many will share this view that the new Bill is the essence of Nick Clegg's 'snooper's charter', namely the legalisation of 'mass surveillance' as it is often described in sections of the media.

Questions about the oversight process

It should be the case that such fears are at least partially allayed by an effective intelligence oversight process. Within Parliament, potential concerns over the role and effectiveness of the parliamentary ISC committee are still matters of debate.

It is true that the Justice and Security Act of 2013, passed under the coalition government, did make some changes to the process of oversight. It is arguable, however, whether these changes amounted to much more than extending the range of intelligence community actors into whose activities

26 Home Office call for consultation on the draft Investigatory Powers Act, retrieved from www.gov.uk/government/consultations/investigatory-powers-act-2016 [accessed 2 August 2018].

27 Jen Stout (2017) 'It's not just "fringe groups" that are at risk of surveillance – UK civil society needs to learn digital security, and fast', *Civil Society Futures*, 25 July 2017, retrieved from https://civilsocietyfutures.org/not-just-fringe-groups-risk-surveillance-uk-civil-society-needs-learn-digital-security-fast/ [accessed 28 September 2018].

the ISC could apply scrutiny to encompass the police and other public bodies. It is still the case that the Prime Minister has to approve all appointments to the committee, in consultation with the Leader of the Opposition, and in this way the committee still does not function in exactly the same way as other Parliamentary select committees. It is interesting to note that it took almost six months after the general election in 2017 to approve all of the newly appointed members of the ISC and for it to meet for the first time; a delay which was almost certainly because of political arguments over who should be on the committee between the Prime Minister, whose majority had been lost in the election, and a combative Leader of the Opposition.

These factors concerning appointments add to the general suspicion in some quarters that the ISC is too close to the establishment in that its members are generally expected to have prior experience of dealing with intelligence matters, usually in the shape of having been ministers of state in the past (although they cannot be a serving minister at the time of their appointment). This means that they may be more sympathetic to the needs of the intelligence services than would a committee member with no prior experience. As Defty argues, they might be reluctant to 'ask difficult questions'.[28] The contrast with the system for appointing oversight committee members in some other democratic countries, such as the US, the Netherlands, and Germany, for example, is marked in this respect. However, a counter-argument would be that there are already problems with committee members not always having the relevant technical expertise to be able to ask the right questions of the security services or indeed to understand which questions to ask at all, a problem shared by Germany and the UK in recent years, to name two.[29] A lack of experience in committee members of intelligence matters may make these problems worse.

The verdict of both Gill[30] and Phythian[31] on the ISC's performance in the pre-Snowden years was mixed. Both acknowledged that the ISC was

28 Andrew Defty (2015) 'It is time to adopt a different approach to appointing members of the Intelligence and Security Committee', *Democratic Audit UK*, 24 March 2015, retrieved from http://eprints.lse.ac.uk/63151/1/democraticaudit.com-It%20is%20time%20to%20adopt%20a%20different%20approach%20to%20appointing%20members%20of%20the%20Intelligence%20and%20Security%20Commi.pdf [accessed 5 September 2018].

29 Marcel Fürstenau (2013) 'Chancellery finds it hard to be transparent about intelligence', Deutsche Welle television website, 25 July 2013, retrieved from www.dw.com/en/chancellery-finds-it-hard-to-be-transparent-about-intelligence/a-16974776 [accessed 4 August 2018].

30 Peter Gill (2007) 'Evaluating intelligence oversight committees: The UK's Intelligence and Security Committee and the "war on terror"', *Intelligence and National Security*, 22(1), pp.14–37.

31 Mark Phythian (2007) 'The British experience with intelligence accountability', *Intelligence and National Security*, 22(1), pp.75–99.

essentially established to 'serve the establishment'[32] and that it could perhaps be criticised for 'resting too comfortably in the warm embrace of the Whitehall village'.[33] At the same time, the ISC was having to design an effective culture of oversight when none to speak of had existed before, and when there were very few clues in the 1994 Intelligence Services Act as to how it should be done.[34] In Gill's eyes at least, the ISC had in its early years somewhat, 'exceeded … expectations'.[35] It had taken on for itself some degree of operational scrutiny, even though this was not technically part of its mandate until 2013, and it had produced some reasonably probing reports into such issues as the Mitrokhin affair, the intelligence concerning Iraqi weapons of mass destruction and the treatment of detainees at Guantanamo Bay.

In the post-Snowden environment, the verdict on the ISC could be said to be similarly mixed. It is the case that the ISC undertook immediate action to investigate allegations of illegality on the specific question of the PRISM programme following Snowden's revelations (eventually ruling in favour of the government). The subsequent breadth of the Privacy and Security Inquiry, which published its findings two years later, undoubtedly provided one of the most significant inputs to the drafting of the new Bill.

In other ways, however, the ISC is almost inevitably somewhat toothless, with a mandate to complain when things go wrong but no power to see any action necessarily result. Although not a concern arising directly from Snowden's revelations, the ISC noted in its report on the UK-authored drone strikes in Syria in September 2015 that the failure by the government to make available to its inquiry a number of sensitive documents had been 'profoundly disappointing' and, 'had a significant bearing on the conclusions'.[36] These are fairly damning words to level at

32 Ibid, p.95.

33 Peter Gill (2007) 'Evaluating intelligence oversight committees: the UK's Intelligence and Security Committee and the "war on terror"', *Intelligence and National Security*, 22(1), p.31.

34 Mark Phythian (2007) 'The British experience with intelligence accountability', *Intelligence and National Security*, 22(1), p.97.

35 Peter Gill (2007) 'Evaluating intelligence oversight committees: the UK's Intelligence and Security Committee and the "war on terror"', *Intelligence and National Security*, 22(1), p.32.

36 Intelligence and Security Committee (2017) 'UK lethal drone strikes in Syria', report presented to Parliament, HC 1152 (26 April 2017), retrieved from https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20170426_UK_Lethal_Drone_Strikes_in_Syria_Report.pdf?attachauth=ANoY7cqiN6Vo8t_OSaAu-0a6JxwENqZkj8StzUbkNkK5Ocq8QqCrI10LftMLGukhmPV0FCkezSKV53m25mVsgJL8AYOJSW0-4g0I1ovIECiGJH1HAdw2jUA5w3172FyuBwKgQkxO4Nqd_WAWAgwybXO-Imnz_zUNPOGkg_hZLJf4SB5AdtgKK20rKk-DufLhL4_wN2MnpsoCKI0gPJdgVre45nQm1XwO9TPk-pZS3vBm4t-QpqVNK2rXo_35XilF5njvTD71iusrgchHWwe-ZsgtfC3OfQgkqw%3D%3D&attredirects=0 [accessed 5 April 2018] p.3.

AU: The url in note 36 appears to be broken. Please provide a shorter url if available.

the executive and make for uncomfortable headlines, but this seems to be where the matter remains in the absence of any substantive response. More pertinently, when the Investigatory Powers Tribunal ruled that data sharing arrangements between GCHQ and NSA under the latter's PRISM programme were insufficient to protect human rights between 2007 and 2014,[37] doubts inevitably persist in some quarters that the ISC is either unwilling to censure the security services or has insufficient access to information within the agencies it is supposed to be overseeing.[38] It is true that this ruling still did not establish illegality as such on the part of the intelligence agencies, but it could reasonably be said to mark a perhaps somewhat disingenuous withholding of information from those who did not know the right questions to ask. As mentioned, the UK is not the only country where there are concerns about the ability of the oversight regime to effectively do battle with smart intelligence services, but it is fair to say the ISC may still have some distance to travel when it comes to the UK's particular environment of oversight.

Conclusions

Did Snowden's revelations in the summer of 2013 initiate a process that resulted in changes to surveillance law in the UK? The answer is that they did not entirely. Concerns about the ability of the security services to continue to be able to access communications data in the changing technological environment and contrary concerns about rights to privacy in the digital age in advanced national security states, were both well underway and leading to a vigorous public debate before Snowden appeared on the scene.

In other ways, however, there is no doubt that Snowden added materially to a growing sense of the need for reliable accountability and oversight of the intelligence services that had been gathering pace since the end of the Cold War. A counterfactual analysis is not available, but it seems doubtful that the UK would have initiated such a major inquiry into the right balance between privacy and security had Snowden not acted as he did. The feverish atmosphere in the immediate aftermath of the revelations probably paved the way for the three heads of the UK intelligence

37 Owen Bowcott (2015) 'UK-US surveillance regime was unlawful "for seven years"', *The Guardian*, 6 February 2015, retrieved from www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa [accessed 4 April 2018].

38 Alan Travis (21015) 'ISC report acknowledges failings but paves way for snooper's charter', *The Guardian*, 12 March 2015, retrieved from www.theguardian.com/us-news/2015/mar/12/intelligence-agencies-finally-understand-need-to-step-out-of-the-shadows [accessed April 2018].

agencies to give open evidence to the ISC for the first time in a session streamed (not quite live) on the internet in October 2013. The ISC itself noted that this was, 'a very significant step forward in terms of the openness and transparency of the Agencies'.[39] It may also be the case that the new IPA Bill would not have been subjected to such a rigorous and comprehensive degree of debate and scrutiny without the Snowden effect. This is not to comment on whether or not he should have acted as he did, but merely to consider the effects.

Two of the key philosophical debates here are where the limits of the state's surveillance powers should be drawn and how far or otherwise we can trust those charged with keeping us safe to do so in a legal and proportionate way. On the latter, David Omand is clear that the intelligence personnel, some of whom he previously directed, should be largely above suspicion. He suggests that, 'it is difficult to overstate the overall impact in recent years of … legislation on the ethos of the UK agencies in creating a disciplined culture within the agencies, while enabling them to carry out a full range of intelligence gathering operations for authorized purposes'.[40] If we couple this with David Anderson's contention that the passage to the new IPA was an exercise in how good law should be conducted in a modern democracy, then we should all feel reasonably reassured. Clearly, however, this does not convince everyone, and situations such as the ISC's recent report on potential complicity by UK intelligence agencies in the torture of terrorist suspects in the post-9/11 era will do nothing for building public trust in those agencies.[41]

Some will be of the opinion, however, that many of those on the civil liberties side of the equation will consider *any* discussion about the legal model for state surveillance to be moot, since they are fundamentally opposed to the central principle of extensive state surveillance capabilities. A terse exchange during the Privacy and Security Inquiry between the civil rights group Big Brother Watch and Hazel Blears MP, a member of the ISC, was indicative in this respect. Big Brother Watch wrote to the ISC on 13 March 2015 in fairly robust terms, complaining about what they felt was a misrepresentation of their evidence given to the Privacy and Security

39 Intelligence and Security Committee (2013) 'Open evidence session' (23 October 2013), retrieved from http://isc.independent.gov.uk/news-archive/23october2013 [accessed 18 July 2018].

40 David Omand (2012) *Securing the State*, Oxford: Oxford University Press, p.284.

41 Intelligence and Security Committee (2018) 'Detainee mistreatment and rendition: 2001–2010', report presented to Parliament, HC 1113, 28 June 2018, retrieved from https://fas.org/irp/world/uk/isc-detainee.pdf [accessed 29 June 2018].

Inquiry.[42] They claimed that Hazel Blears had stated in a press conference following publication of the inquiry report that:

> some of our witnesses considered that it is preferable to allow some terrorist attacks to happen rather than to allow any form of bulk interception.[43]

This, claimed Big Brother Watch, was a dangerous misrepresentation of a response given to a question during the inquiry hearings. In response to a demand for an immediate public correction of this point, Blears stuck to her guns about the way in which Big Brother Watch's comments had been rendered in the report and suggested that they should have said earlier if they wished to clarify any of their statements.[44] She noted that:

> If Big Brother Watch wishes to clarify its position in respect of whether bulk interception is unacceptable in a free society even if it leads to terrorists being prevented from carrying out attacks, then we would be happy to note that position.[45]

While critics of the government could consider this to be an emotionally charged mechanism for discrediting any position of opposition to bulk surveillance powers, it does throw down the gauntlet as to how, exactly, successful national security can and should be delivered in the modern environment of threat and communications behaviours. There does appear to be a paucity of ideas on how this could be done, other than an implicit suggestion of a completely surveillance-free utopia. It is also the case that current technology does not appear to support any model whereby terrorists and criminals are surgically discriminated from the rest of the population ahead of time. It may be that advances in big data technology will allow such actions in time, but they do not do so at the time of writing.

42 The letter was issued by Renate Samson, Chief Executive of Big Brother Watch, and addressed to the Senior Assistant Clerk to the ISC, 'in the absence of the Committee having a Chair'. (The correspondence fell between elections at a time when the ISC's chair and members had not yet been officially reappointed.) All related correspondence can be seen on the ISC website retrieved from http://isc.independent.gov.uk/news-archive/17march 2015 [accessed 8 August 2018].

43 Ibid.

44 Intelligence and Security Committee (2015) response letter to Renate Samson, Chief Executive of Big Brother Watch, from Hazel Blears MP, 17 March 2015 (Ref: ISC 4.21/146).

45 Ibid.

Perhaps ironically for Snowden's supporters, the new IPA Bill that resulted from the debates he substantially punctuated, does not claw back surveillance powers from the state but further consolidates them to a large extent. It is true that the authorisation process for content interception has been substantially strengthened, and the oversight commissioner function has been streamlined and simplified, but in other ways, the legal regime covering all surveillance activities has had further complexity added to it. This is not necessarily a deliberate attempt to make things as difficult as possible for the scrutineers, and may be as much about the incredible complexity of surveillance in the modern digital age as about any nefarious agency. But it leaves open the question as to whether more legal streamlining will be necessary in the future.

Similarly, what has not been achieved is any greater clarity about the rights to privacy in the digital age and the proper boundaries to state surveillance in the new environment. It is interesting to note that more recent debate has swung slightly away from states themselves and towards the big data activities of the major CSPs, who have now reached sufficient size and profit that they rival the GDP of many states. Indeed, the purported founder of the internet, Tim Berners-Lee, for example, has targeted the big social media companies in his concerns about global governance of the internet[46], having previously been a vocal critic of the UK's 'snooper's charter'.[47] There is a logic in that Berners-Lee would rather see measures for promoting good governance on the internet than unfettered abilities to control and manipulate it for information gain. But while the debates continue about the proper boundaries of privacy and security, advanced states such as the US and UK have made sure they continue to have substantial capabilities in the digital domain, and to make sure these are enshrined in law.

46 Tim Berners-Lee (2018) 'The web can be weaponised – and we can't count on big tech to stop it', *The Guardian*, 12 March 2018, retrieved from www.theguardian.com/commentisfree/2018/mar/12/tim-berners-lee-web-weapon-regulation-open-letter [accessed 4 April 2018].

47 Alex Hern (2015) 'Tim Berners-Lee urges Britain to fight "snooper's charter"', *The Guardian*, 29 May 2015, retrieved from www.theguardian.com/technology/2015/may/29/tim-berners-lee-urges-britain-to-fight-snoopers-charter [accessed 5 May 2018].