Snooper's Charter? Reflections on 2016 update to interception law in the UK

Julian Richards[1], University of Buckingham

PSA, Cardiff, 2018

Abstract: In 2016, Parliament passed into law the Investigatory Powers Act (IPA), commonly referred to in the media as the "Snooper's Charter". The new law reflected the twin pressures of a post-Snowden environment of scrutiny and concern about the nature and extent of the UK's interception powers; and a recognition that changes in technology were changing the interception and surveillance landscape. For civil libertarians, the frequently used moniker of "Snooper's Charter" for the new law reflected a concern that it essentially gave the state a blank cheque for extending and deepening surveillance into private individuals' communications, including their internet-based activity. Concerns were also raised about the effective rubber-stamping of "bulk access" interception exposed by Snowden; and a mandate apparently being given for state-sponsored computer hacking. Counter-arguments include the fact that the new law would probably not have happened had it not been for Snowden and other whistleblowers, and that it offers increased accountability of surveillance operations in the modern communications environment. This paper critically reviews the assessments on both sides of the fence.

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, the Guardian newspaper in the UK published the first of a set of hitherto highly classified revelations derived from his documents. The details implicated not only the NSA in industrial-scale interception and collection of global communications, but also its key signals intelligence (Sigint) partner in the UK, GCHQ, at a scale and method that were, it was implied,

[1] Co-director of the Centre for Security and Intelligence Studies (BUCSIS), University of Buckingham. Julian.richards@buckingham.ac.uk

both hugely disproportionate and potentially unlawful. On 9 June, Snowden went public for the first time with an interview aired on the internet in which he claimed that "he had done nothing wrong"[2]. 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, where he remains at the time of writing.

The impact of the revelations on the intelligence operation 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[3], 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 DNI at the time, James Clapper, told the Senate Intelligence Committee that Snowden's revelations had caused "grave damage" to the intelligence operation[4]. 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 on the list of nominees for the European Parliament's Sakharov Prize for Freedom of Thought, by claiming that he had pondered whether there was actually a different list that might more appropriately bear Snowden's name. (Hayden did stress afterwards that he never meant to imply Snowden should be on any sort of kill list!)[5] 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 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 going about their business. 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 whistleblowers, 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 in Moscow on his arrival was Jesselyn Radack, the US-based civil rights

[2] https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline
[3] Cited in Hayden 2014
[4] Cited in Weinstein 2014, p.5
[5] Hayden, 2014

lawyer, who travelled to the Russian capital to present Snowden with an "Integrity in Intelligence" award[6].

The road to the Investigatory Powers Act 2016, or "Snooper's Charter"

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[7]. In large part, the debate was already being driven by the twin but not entirely complementary pressures of changes in technology that were making traditional approaches to Sigint more difficult; and the massive explosion of personal data in cyberspace that seemed to raise extremely complex and ambiguous questions about the rights to, and boundaries of privacy.

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 a simmering one for some time, since it was increasingly being recognised that changes in technology; in communications network configurations and in communications behaviours, were leading to a gradual dwindling in the amount of communications data the police and intelligence services could access to support their investigations into matters of national security. In particular, the rise of bundled contracts for consumers in which communications events were charged not by individual events but within general tariffs was meaning that the communications service providers (CSPs) were increasingly no longer planning to keep the sort of data traditionally characterised as "billing records", since there was no need to do so. The problem for the security agencies in the disappearance of these records (generally considered 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 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 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[8].

Thus was commenced deliberations about a new bill initially called the Communications Data Bill, which evolved into the wider Investigatory Powers Act (IPA) in 2016. The beginning of the journey

[6] Foreign Policy 2013, p.67
[7] Hayden 2014, p.14
[8] ISC February 2013, p.8

towards the realisation of this new law, however, starts some time before Snowden's revelations. Indeed, it is appropriate to go slightly further back to the general elections of 2010 to identify where the issue had started to become particularly problematic. In these elections, 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 saw himself as something of a gatekeeper to the more surveillance-minded instincts of some of his Conservative colleagues, warning that the new bill "won't happen while Lib Dems are in government"[9].

The competing forces of a desire by security agencies to capitalise on Big Data to support investigations, against a disquiet in civil society about privacy protections in the internet age, was already becoming complicated, but it is fair to say that Snowden's revelations a few months after the ISC's February 2013 report further complicated the situation. Whether his revelations were pivotal to the picture, or were just a bump in a road already travelled, is the key question to which we will return.

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); an act passed in 1975 following the Church Committee inquiry, which 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 can also be used on suspected terrorist targets using US-based CSPs.) Because the Snowden files revealed that GCHQ had also had extensive access

[9] http://www.alphr.com/politics/22986/lib-dems-block-snoopers-charter accessed 13 March 2018

to such FISA-authorised data since 2007 through a system called PRISM, 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[10]. Following extensive scrutiny of GCHQ files and processes, the ISC concluded robustly in July 2013 that no illegal access to such communications had taken place[11].

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 an extensive investigation called 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); in addition to 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 European Court of Justice (ECJ) playing a key role. This cycle is continuing at the time of writing.

By 2014, the government found itself facing three problems concerning continued access to communications data. The first was the technology problem described above, whereby the security agencies were becoming increasingly concerned about a declining lack of access to the data they felt they needed. 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 proposed new Communications Data Bill. To these two challenges was added a judgement in the ECJ, which suggested that the UK's current practice in this area, as defined by 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). This, it was suggested, meant that UK law was not providing sufficient protection of privacy under the 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

[10] ISC July 2013, p.1
[11] Ibid

parliament by the Home Secretary, Theresa May, on 10 July 2014[12]. 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, such that a new, over-arching law could be put in place. A year later, the Conservatives established an overall majority at the general elections and were 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 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 seems to cut 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"[13].

The government appealed the decision, and, in April 2016, it went to the ECJ in Luxembourg, to be heard alongside a similar case involving a proposed new law in Sweden, and taking into account an earlier case limiting the collection of data, known as Digital Rights Ireland[14].

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"[15]. Both reports informed the drafting of the new IPA bill, which commenced pre-legislative scrutiny in March 2016, and received Royal Assent in November of that year having successfully passed through both houses of parliament.

[12] https://www.gov.uk/government/speeches/communications-data-and-interception accessed 13 March 2018
[13] https://www.theguardian.com/world/2015/jul/17/data-retention-and-surveillance-legislation-ruled-unlawful accessed 13 March 2018
[14] https://www.theguardian.com/world/2016/apr/11/european-court-to-consider-legality-of-uk-surveillance-laws accessed 13 March 2018
[15] See https://www.daqc.co.uk/2015/06/11/a-question-of-trust-report-of-the-investigatory-powers-review/ accessed 13 March 2018

One of the key elements of the ISC's "Privacy and Security" report, concerned legislation governing investigatory activities, and specifically the notion that the Regulatory and Investigatory Powers Act (RIPA) of 2000 and related pieces of legislation were both too complex for anyone to easily navigate through, and increasingly 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"[16], which 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 (ibid). The Interception of Communications Commissioner, Sir Anthony May, was less charitable, noting in his 2013 annual report that[17] ".. 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."

Anderson's "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"[18]. Perhaps sharing Sir Anthony May's feelings, the Anderson report noted that[19]:

> "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."

Where David Anderson went much further, however, was 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[20]. Such a suggestion would mark a significant departure from, and strengthening of intelligence authorisation processes, albeit in the more highly

[16] ISC March 2015, p.2

[17] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/302597/InterceptionCommunicationsCommissionerPrint.pdf, p.61

[18] https://www.daqc.co.uk/wp-content/uploads/sites/22/2015/06/IPR-Report-Print-Version.pdf, p.4

[19] https://www.daqc.co.uk/wp-content/uploads/sites/22/2015/06/IPR-Report-Print-Version.pdf, p.8

[20] https://www.daqc.co.uk/wp-content/uploads/sites/22/2015/06/IPR-Report-Print-Version.pdf, p.7

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 managed to lose her parliamentary majority in the general elections 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 ECJ 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[21]. At the time of writing, the government is considering its response to this legislative conundrum.

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 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 state hacking), had been acted upon[22]. 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

[21] https://www.theregister.co.uk/2016/12/21/eu_judgment/ accessed 13 March 2018

[22] https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20160209_ISC_Press_Release_IPBill.pdf?attachauth=ANoY7cqfn1qzYnl5MUnccyiQZvdKMExbrf9xIu99ai_0fmOdGPONgzEvJqF1zH7IT9il1Wzh_orzsBnmUFJQktGZF-hQL6rcuAmvR9BHm9XHAQfB0txcHgRinu_G8gm9SmYOICnSvPwlH0ZGzNfMinsrvxPE2U6tSU8kond9hfkLnC4MY-UZzKl8StcQw4hMpRwxSDCcFFnhqqVg1e4wUp4f8NfLHJxGsK4Zuh3k4Dq0KtJcbOXsIu-4tU2tQNX5CaghwUKjGGk8&attredirects=0 accessed 13 March 2018

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"[23].

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[24].

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 privacy protections in the modern democracy.

However, Anderson was himself much more positive about the new law. Issuing a statement on his webpage entitled "The Investigatory Powers Act 2016 – an exercise in democracy", he noted that the Act "gets the big things right", and that more than 90 percent of the recommendations in his "Question of Trust " report had been enacted[25]. Indeed, he observed that that the new law was "one of the most carefully-scrutinised laws of recent times" and concluded that the result was "a victory for democracy and the rule of law"[26].

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. Many 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. In Germany, the revelations led to an ad hoc cross-parliamentary inquiry, called the "NSA Inquiry" (*Untersuchungsausschuss* ,NSA) launched in March 2014. This inquiry uncovered concerns and weaknesses in the authorisation process for 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

[23] Ibid
[24] Ibid
[25] https://www.daqc.co.uk/2016/12/03/the-investigatory-powers-act-2016-an-exercise-in-democracy/ accessed 14 March 2018
[26] Ibid

judicial oversight system"[27], but introduced new confusions and gaps in the oversight machinery, leaving parliamentary oversight of intelligence "fragmented"[28].

Indeed, 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.

The current situation

At the time of writing, the IPA has passed into law in the UK and is being observed, albeit with a new challenge on the table from the ECJ about whether authorisation of bulk communications data requests should be strengthened. The new law does not provide the grand, over-arching and simplified surveillance law that the ISC wanted, but could actually be argued to have increased the legislative complexity by leaving some activities still subject to the pre-existing RIPA law (notably Humint authorisation and covert surveillance operations), while interception and computer network exploitation now have a new law. Conversely, the oversight regime has been streamlined to large extent, with a single commissioner's office (the Investigatory Powers Commissioner's Office; IPCO) replacing the three separate offices that existed previously. This is a major step forward for all concerned.

In terms of how the law 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 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 brought in 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

[27] Wetzling 2017, p.3
[28] Ibid, p.25

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 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 ECJ'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 ECJ. 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: a system sometimes described as "double-lock" authorisation. For communications data, however, the former level of authorisation has been retained, namely a "bulk access" authorisation such that individuals 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 ECJ has 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, as 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[29]. 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

[29] ISC, February 2013, p.7

year. The government has proposed some changes to the IPA and taken the unusual step of laying these proposals out for consultation[30], although it is fair to say that the ECJ'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, while still largely appearing to balance civil fears about privacy.

For some in the field of civil liberties, however, this is not a great outcome, and means that the questions posed by Snowden about the reach of the most powerful national security states have not been suitably 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"[31]. 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 should be 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. In particular, the status of the ISC changed nominally to that of a full parliamentary select committee (rather than a more limited committee of appointed parliamentarians as had been the case before); and the remit of the committee to be able to look into operational as well as functional processes within the intelligence services was formally established. The range of intelligence community actors

[30] https://www.gov.uk/government/consultations/investigatory-powers-act-2016 accessed 19 March 2018
[31] https://civilsocietyfutures.org/not-just-fringe-groups-risk-surveillance-uk-civil-society-needs-learn-digital-security-fast/ accessed 19 March 2018

into whose activities the ISC could apply scrutiny was also expanded to encompass the police and other public bodies.

However, a counter-argument would be that these changes have meant very little in practice. 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 exactly the same way as other parliamentary select committees. It is interesting to note that it took almost six months after the general elections 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 elections – 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 be a committee member with no prior experience. As Defty argues, they might be reluctant to "ask difficult questions"[32]. The contrast with the system for appointing oversight committee members in some other democratic countries, such as the US, the Netherlands or 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 arguably shared by Germany and the UK in recent years[33]. A lack of experience in committee members of intelligence matters may make these problems worse.

The verdict of both Gill[34] and Phythian[35] on the ISC's performance in the pre-Snowden years was mixed. Both acknowledged that the ISC was essentially established to "serve the establishment"[36]and, that it could perhaps be criticised for "resting too comfortably in the warm embrace of the Whitehall village"[37]. At the same time, the ISC was having to design an effective

[32] 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 19 March 2018
[33] See for example: http://www.dw.com/en/chancellery-finds-it-hard-to-be-transparent-about-intelligence/a-16974776 accessed 19 March 2018
[34] Gill 2007
[35] Phythian 2007
[36] Phythian, ibid, p.95
[37] Gill, ibid, p.31

culture of oversight when none to speak of had existed before, and when there were very few clues as to how to do it in the 1994 Intelligence Services Act[38]. In Gill's eyes at least, the ISC had in its early years somewhat "exceeded … expectations"[39]. It had taken on for itself some degree of operational scrutiny, even though this was not technically part of its mandate until 2013, and 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 again be said to be somewhat 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 from such complaints. Although not a concern arising directly from Snowden's revelations, the ISC noted in its report on the 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" reached[40]. 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[41], 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[42]. 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 on these issues.

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

[38] Phythian, ibid, p.97
[39] Gill, ibid, p.32
[40] ISC April 2017, p.3
[41] https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa accessed 19 March 2018
[42] https://www.theguardian.com/us-news/2015/mar/12/intelligence-agencies-finally-understand-need-to-step-out-of-the-shadows accessed 19 March 2018

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.

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 had initiated such a major inquiry into the right balance between privacy and security had Snowden not spoken. The feverish atmosphere in the immediate aftermath of the revelations probably paved the way for the three heads of the UK intelligence 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"[43]. 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 done what he did, but merely to consider the effects.

Perhaps ironically for Snowden's supporters, the new IPA bill that has resulted from these debates does not claw back surveillance powers from the state, but actually further consolidates them to a large extent. 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. But it leaves open the question as to whether more 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. It is interesting that the purported founder of the internet, Tim Berners-Lee, for example, has targeted the big social media companies in his latest salvo of concerns about global

[43] http://isc.independent.gov.uk/news-archive?offset=30 accessed 19 March 2018

governance of the internet[44], having previously been a vocal critic of the UK's "snooper's charter"[45]. There is a logic, in that Berners-Lee would rather see measures for promoting good governance on the internet than measures to control and manipulate it for information gains, 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.

[44] https://www.theguardian.com/commentisfree/2018/mar/12/tim-berners-lee-web-weapon-regulation-open-letter accessed 19 March 2018

[45] https://www.theguardian.com/technology/2015/may/29/tim-berners-lee-urges-britain-to-fight-snoopers-charter accessed 19 March 2018