Statement Requested by the Bundestag Committee of Inquiry Investigating the Revelations by Edward Snowden Regarding Internet and Telecommunications Surveillance: The Public Debate in the United Kingdom

Ben Hayes, 1 July 2015

I INTRODUCTION

1. I am a Fellow of the Amsterdam-based Transnational Institute and a freelance researcher and consultant on security and human rights matters resident in the United Kingdom.[1] I have been asked to provide the Committee with "a detailed description of the debate which has taken place in parliamentary, public and academic spheres in the United Kingdom since the revelations made by Edward Snowden on issues concerning the activities of UK's own intelligence services, the parliamentary oversight of these activities and the protection of privacy, including an overview of important documents, statements or other information published by the government, parliament, NGOs or other players in this field."

2. To this end my statement contains six substantive sections addressing the following matters: (i) the position of the UK government on the Snowden revelations (paragraphs 3-22); (ii) related developments that have widened the debate about surveillance (paragraphs 23-42); (iii) inquiries and reviews by the UK parliament and other significant actors (paragraphs 43-68); (iv) judicial review and surveillance reform (paragraphs 69-84); (v) civil society campaigns (paragraphs 85-100); and (vi) the significance of this information for Germany (paragraphs 101-107).

II THE POSITION OF THE UK GOVERNMENT ON THE SNOWDEN REVELATIONS

3. This section sets out the government's response to the revelations by Snowden and its position on key policy deliberations. It is pertinent to analyse the public debate from this starting point because, following a short period of 'damage limitation', the debate has been increasingly shaped by the public positions that the government and its security agencies have taken.

Preliminary observations

4. It has been argued that the UK government has been able to shape and contain public debate because it has been well-served by a largely compliant mainstream media which has, with but a few notable exceptions, provided relatively little coverage of the Snowden revelations and the issues of fundamental rights and democratic governance that they raise. Dr Arne Hintz of Cardiff University's School of Journalism, Media and Cultural Studies suggests, for example, that "Newspapers like the Times and the Daily Telegraph accused the Guardian [which published the initial Snowden revelations] of threatening the security of the

[1] Over the past 20 years I have also been employed by the London-based civil liberties organisation Statewatch, the European Center for Constitutional and Human Rights in Berlin, the Human Security Collective in The Hague, the Peace Research Institute Oslo, and Trilateral Research and Consulting. My research and consultancy has included work for, among others, the European Commission, European Parliament, the United Nations, the International Federation of Journalists, the International Committee of the Red Cross, and the Open Society Foundations.

country and thereby placed themselves at the service of the government and the spy agencies. The BBC coverage was limited, at best. Whereas the revelation on September 20th [2013] that the British secret service had hacked into the Belgian telecom operator Belgacom to spy on EU institutions raised a lot of interest outside the UK, the BBC failed to report it at all".[2]

5. Successive governments have also received tacit support from the major opposition parties, whose criticism has been muted at best – again with notable exceptions from within their ranks – and the substantive findings of the UK Investigatory Powers Tribunal (IPT), the judicial body in the UK that hears complaints from members of the public about surveillance), which has for the most part upheld the legality of Government Communications Headquarters (GCHQ) policy and practice (see further para. 70-72). The emergence of the "Islamic State" and the decision of hundreds of British nationals to join that group coupled with a relentless government and media focus on 'radicalisation', particularly 'online radicalisation', has also been used to legitimise and garner public support for government surveillance powers (see further para. 40-42).

6. Whereas many people outside of the UK are interested in the apparent mismatch between the magnitude of what Snowden revealed and a perceived lack of public and political concern on the part of the British public – at least as compared to countries such as Germany – I would submit that the political culture of deference to the security apparatuses in the UK may be unique among states with comparable democratic and legal traditions. The impact of the Snowden revelations should not in my view be seen in isolation, but considered in the context of largely unmitigated security service impunity for unlawful conduct during many decades of UK counter-insurgency operations in its former colonies, against Irish Republicanism in the North of Ireland, and more recently in its prosecution of the so-called "war on terror". I concur with Sir Stephen Sedley, a former Court of Appeal Judge, who commented in the wake of the Snowden revelations, that the security apparatus is "able to exert a measure of power over the other limbs of the state that approaches autonomy: procuring legislation which prioritises its own interests over individual rights, dominating executive decision-making, locking its antagonists out of judicial processes and operating almost free of public scrutiny".[3]

7. It also appears that few, if any, members of the executive branch of government were aware of the extent of surveillance by the UK intelligence agencies[4] prior to the Snowden revelations. According to Chris Huhne, a government minister at the time of the disclosures, the cabinet was "told nothing about GCHQ's Tempora or the NSA's Prism, or about their extraordinary capability to vacuum up and store personal emails, voice contact, social networking activity and even internet searches". Huhne, who was also a member of the UK National Security Council which is attended by ministers and the heads of the secret and security services, GCHQ and the military, also stated: "I do not know whether the prime minister or the foreign secretary (who has oversight of GCHQ) were briefed, but the NSC was

[2] "Snowden, the Media and Surveillance: Looking back at the Leak of the Year", 18 December 2013, available at: http://www.jomec.co.uk/blog/snowden-the-media-and-surveillance-looking-back-at-the-leak-of-the-year/.
[3] "Beware Kite-Flyers", London Review of Books, 12 September 2013, available at: http://www.lrb.co.uk/v35/n17/stephen-sedley/beware-kite-flyers.
[4] The term 'intelligence agencies' refers collectively to the Security Service (MI5), the Secret Intelligence Service (MI6) and the Government Communications Headquarters (the UK's signal intelligence agency - GCHQ).

not".[5] That the UK's political system lacks the capacity and experience of holding its most powerful and secretive agencies of state to account with much more than a 'rubber-stamp' should not in my view be held synonymous with apathy or indifference on the part of the public as a whole.

"Neither confirm nor deny"

8. For decades "neither confirm nor deny" (NCND) has been the stock response of government ministers and officials when questioned on the activities of the UK's intelligence agencies. The very existence of GCHQ was not officially acknowledged until the early 1980s and the agency was not regulated by law until the Intelligence Services Act of 1994. NCND has been routinely invoked in response to questions raised by documents leaked by Snowden, and is frequently paired with blanket reassurances that the intelligence agencies always act within the law. This stance appears doubt in the minds of the public as to the gravity and veracity of Snowden's revelations.

9. The government was even able to maintain its "neither confirm nor deny" stance during the Investigatory Powers Tribunal (IPT) proceedings in respect to its "Tempora programme", meaning that the IPT could only rule on whether Tempora would hypothetically be permissible under UK law (see further para. 70-72).

10. The government has however had to concede some ground and acknowledge the existence of various practices revealed by Snowden. In respect to the sharing of data with foreign intelligence agencies, including the United States' National Security Agency (NSA), the government was forced to reveal to the IPT that the arrangements are extremely permissive (see further para. 90-91). UK intelligence agencies can receive and request large quantities of "unanalysed" bulk data without a warrant whenever it would "not be technically feasible" for them to acquire the information themselves. This 'foreign intelligence' material – comprising both the metadata and content of communications – could then be kept on a large searchable database for up to two years, access to which would not be regulated by the Regulation of Investigatory Powers Act 2000 (RIPA), the UK's principle surveillance statute.[6]

11. Another key admission came in the witness statement of Charles Farr, the Director General of the Office for Security and Counter Terrorism at the UK Home Office. Farr confirmed that all communications sent through web-based platforms outside the UK are treated as "external communications" under RIPA. This is important because RIPA imposes a legal distinction between "internal" and "external" communications. In effect, RIPA mandates that internal surveillance must be 'targeted' (albeit loosely), whereas external surveillance can be indiscriminate or 'blanket'.[7] These provisions are analogous to arrangements in the

[5] "Prism and Tempora: the cabinet was told nothing of the surveillance state's excesses", Guardian, 6 October 2013, available at: http://www.theguardian.com/commentisfree/2013/oct/06/prism-tempora-cabinet-surveillance-state.

[6] "Secret policy reveals GCHQ can get warrantless access to bulk NSA data", Liberty, 29 October 2014, available at: https://www.liberty-human-rights.org.uk/news/press-releases/secret-policy-reveals-gchq-can-get-warrantless-access-bulk-nsa-data.

[7] Internal communications can be intercepted only with a section 8(1) warrant from the Home Secretary, which is issued on suspicion of criminal activity and must specify the subject of the interception or a single set of premises. The interception of external communications require a section 8(4) warrant which can be issued only if the Home Secretary feels the surveillance to be necessary and which does not require the intended target of the interception to be specified.

US, which provide safeguards in respect to the internal communications of US citizens while allowing dragnet foreign surveillance under section 702 of the Foreign Intelligence Surveillance Act. Crucially, however, Farr's evidence confirmed that based on the government's definition of what constitutes an "external communication", almost all communications sent via social networking sites such as Facebook and Twitter, Google searches, YouTube, webmail services such as Gmail, Yahoo and Hotmail, as well as emails to or from non-British citizens abroad, can be broadly monitored under the lower, external standard in RIPA.[8] Thus even if both the sender and recipient of a message sent via one of these communications platforms are based in the UK, GCHQ would still consider it an "external communication" (i.e. because non-UK webservers were used to deliver the message). Subject to a ministerial certificate specifying broad justifications, UK intelligence agencies are allowed to read, listen to and look at all of these "external communications". The only ostensible restriction is that they cannot search through this material using "selectors" (keywords or terms) that relate specifically to British citizens or residents. Farr's statement represented an unprecedented admission that British citizens, corresponding via supposedly private channels, are legitimate legal targets for warrantless interception. The UK's Independent Review of Terrorism Legislation has recently suggested that this "loophole" be closed (see para. 62-68).

12. Farr acknowledged the existence of the US's "Prism" and "upstream collection" programmes because they had "been expressly avowed by the executive branch of the US government".[9] Likewise he acknowledged that GCHQ had received information from the Prism programme because this had been confirmed by the Intelligence and Security Committee in July 2013 (see para. 45). There have however been no further admissions or disclosures in respect to the UK's relationship with the US, the "Five Eyes" or any other intelligence partnerships, though the government has gone as far as denying that such arrangements are used to circumvent domestic legal protections. The Home Secretary stated: "It has been alleged that our agencies rely on their counterparts overseas - notably those in the United States - to provide them with intercepted communications unlawfully. This is - quite simply - untrue."[10]

13. The government has maintained its "neither confirm nor deny" position in respect to repeated allegations that GCHQ hacked legal persons located in foreign countries, such as Belgacom and Gemalto, but in February 2015 effectively acknowledged the intelligence agencies' worldwide hacking capabilities for the first time in a Home Office consultation on a draft Equipment Interference Code of Practice. The publication of the code was clearly prompted by pending litigation at the IPT rather than any overarching desire for greater transparency on the part of the government (see para. 75-80). The minister responsible for the code noted that "There are limits on what can be said in public about this work", and claimed that: "The abilities to read or listen to a suspect's communications or to interfere with his or her computer equipment are among the most important, sensitive, and closely scrutinised powers available to the state".[11]

---

[8] I.e. under a section 8(4) warrant under RIPA, supra.

[9] Witness statement of Charles Farr, 16 May 2014, available at: https://www.liberty-human-rights.org.uk/sites/default/files/Witness%20statement%20of%20Charles%20Farr%20on%20behalf%20of%20the%20Intelligence%20Services%2016th%20May%202014.pdf.

[10] "Home Secretary's Defence and Security Lecture", 24 June 2014, available at: https://www.gov.uk/government/speeches/home-secretarys-defence-and-security-lecture.

[11] "Consultation on the draft Codes of Practice on Interception and Equipment", 6 February 2015, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401867/Consultation_on_the_draft_Codes_of_Practice_on_Interception_and_Equipmen....pdf.

14. On all other questions relating to the Snowden revelations, including the involvement of UK intelligence agencies in 'drone' strikes and 'extrajudicial killings' (see para. 38-39), the government has maintained the traditional "neither confirm nor deny" stance for intelligence matters. As suggested above, this has had an important impact on the public debate in the UK. Dr Arne Hintz observes that "A peculiar aspect of much [media] reporting has been a strong caution (to put it mildly) towards the facts (i.e., those undenied and undeniable facts that were revealed in the Snowden leaks) and a complete lack of caution towards claims and beliefs (particularly, those coming from the government and spy agencies), even when the latter were in direct contradiction with the known facts".[12]

"Mass surveillance" and the right to privacy

15. Concomitant to the government's "neither confirm nor deny" policy has been the unequivocal and often preposterous rejection of any notion that GCHQ engages in the practice of mass surveillance. For example, speaking in the aftermath of the initial Snowden revelations, Theresa May, UK Home Secretary, insisted that "there is no programme of mass surveillance and there is no surveillance state". She acknowledged "That some people have alleged that GCHQ is exploiting a technical loophole in legislation that allows them to intercept external communications – that is, communications either sent or received outside the United Kingdom – at will and without authorisation" but argued that such claims were "nonsense… the definition of external communications was set out clearly in the Regulation of Investigatory Powers Act. It is not new, it is not hidden."[13] Giving evidence to Parliament's Intelligence and Security Committee (see para. 44-52) in October 2014, May has also defended the culture of secrecy surrounding the activities of the intelligence agencies and the government's continued "neither confirm nor deny" policy. The European Court of Human Rights has admitted challenges to the UK's bulk interception capabilities and its intelligence agencies' blanket exemption from the UK's freedom of information law (see para. 81).

16. The government also maintains that bulk data collection is not "an invasion of privacy", arguing: "We have to have a haystack to be able to find the needle that we need to keep the public safe."[14] In her evidence to the Intelligence and Security Committee, May argued that bulk data collection did not constitute mass surveillance because "most of the data will not be looked at at all, will not be touched".[15] She also dismissed concerns surrounding overbroad storage of and access to communication data. Privacy considerations, May argued, should only be relevant "at the point at which the communication is opened". She also justified government bulk data collection on the basis that it was in line with the activities of commercial companies who collect large amounts of data on their customers to facilitate targeted advertising. The Committee pointed out that people usually consent to this form of data collection, even if sometimes unknowingly. May countered: "I think there is – not a contract entered into – but an unwritten agreement between the individual and the state that the state is going to do everything they can to keep them safe and secure".

17. In March 2015, the government effectively called for an end to the discussion of the Snowden revelations. Philip Hammond, Foreign Secretary, suggested that the debate about

[12] Supra, note 2.
[13] Supra, note 10.
[14] "Secretive Home Secretary quizzed over UK mass surveillance", Russia Today, 16 October 2014, available at: http://rt.com/uk/196468-may-questioned-security-committee/.
[15] "Theresa May: We need to collect communications data 'haystack'", BBC, 16 October 2014, available at: http://www.bbc.co.uk/news/uk-politics-29642607.

surveillance "cannot be allowed to run on forever" and that it was "quite clear that the ability to intercept bulk communications data, to subject that metadata to electronic analysis and seek to extract the tiny, tiny percentage of communications that may be of any direct security interest does not represent an enhancement of the agencies' powers. Rather it represents an adaptation of those powers to the realities of the 21st century".[16] These repeated claims represent a concerted strategy of systematic denial of the scale and impact of the international communications surveillance revealed by Snowden.

Snowden's revelations have "damaged national security"

18. The government has repeatedly asserted that Snowden's revelations have damaged the national security of the UK – albeit without providing any tangible evidence of such harms. Implicit in the sweeping condemnations of Snowden and the journalists and media outlets with which he worked is a defence of the practices he revealed. Moreover, in shifting the locus of harm from intrusive state surveillance to public fears and anxieties about terrorism, the government has been able to that what is now needed is more surveillance capabilities.

19. In October 2013 the Prime Minister told parliament: "I think the plain fact is that what has happened has damaged national security, and in many ways the Guardian themselves admitted that when they agreed, when asked politely by my national security adviser and Cabinet Secretary, to destroy the files they had, they went ahead and destroyed those files. So they know that what they are dealing with is dangerous for national security."[17] The Guardian offers a different version of events, in which cordial requests to destroy or hand over the data – reportedly along the lines of "You've had your fun: now we want the stuff back"[18] – turned to threats of legal action, at which point the Guardian decided to destroy the files to avoid prior restraint of publication.[19] The paper's then editor, Alan Rusbridger, said: "I explained to British authorities that there were other copies in America and Brazil so they wouldn't be achieving anything… But once it was obvious that they would be going to law I preferred to destroy our copy rather than hand it back to them or allow the courts to freeze our reporting."[20]

20. Following the Prime Minister's intervention, Parliament's Home Affairs Select Committee decided to consider "elements of the Guardian's involvement in, and publication of, the Snowden leaks" as part of ongoing counter-terrorism enquiry (see para. 48). In November 2013, before these proceedings were underway, Sir John Sawers, then head of MI6, told a separate Intelligence and Security Committee enquiry hearing (see para. 49-52) that "The leaks from Snowden have been very damaging. They've put our operations at risk. It is clear our adversaries are rubbing their hands in glee. Al Qaeda is lapping it up." These claims were echoed by the head of MI5 and endorsed by the Home Secretary and Foreign Secretary; meanwhile the former Defence Secretary wrote to the Crown Prosecution Service seeking

[16] "Philip Hammond: time to 'move on' from Snowden surveillance revelations," Guardian, 10 March 2015, available at: http://www.theguardian.com/world/2015/mar/10/uk-must-move-on-from-surveillance-powers-debate-says-philip-hammond.
[17] "David Cameron criticises the Guardian for publishing Snowden data," BBC, 16 October 2013, available at: http://www.bbc.co.uk/news/uk-politics-24555955.
[18] Simon Jenkins, "So the innocent have nothing to fear? After David Miranda we now know where this leads," Guardian, 20 August 2013, available at: http://www.theguardian.com/commentisfree/2013/aug/20/innocent-fear-david-miranda.
[19] "NSA files: why the Guardian in London destroyed hard drives of leaked files", Guardian, 20 August 2013, available at: http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london.
[20] Alan Rusbridger, "The Snowden Leaks and the Public", The New York Review of Books, 21 November 2013, available at: www.nybooks.com/articles/archives/2013/.../snowden-leaks-and-public/.

legal action against the Guardian.[21] At the Home Affairs Committee hearing in December 2013, the Home Secretary was criticised by MPs for failing to provide evidence to support the "melodramatic soundbites" and "highly emotional statements" of the intelligence agencies.[22] The Prime Minister had already vetoed requests from the chair of the Committee for the heads of the agencies to attend the hearings themselves.

21. In April 2014, Charles Farr claimed that ministers have been given "conclusive evidence" of how individual suspects and terror cells have dropped off the intelligence radar since the publication of information on surveillance capabilities and methods: "Our coverage of counter-terrorist activity is not as good as it otherwise might have been".[23] Similarly, in March 2015, Theresa May told MPs: "I assess and so does the director general of MI5 that the Snowden leaks did cause damage. It has had an impact on the ability of our agencies to do the work they need to do. It would be fair to say it has had an impact not just on agencies in the UK. If work has been done to try to mitigate the impact, that uses resources."[24] These assertions have been accepted uncritically by much of the mainstream media. On 14 June 2015 the Sunday Times reported a series of unsubstantiated claims by anonymous government sources about the impact of the Snowden revelations in an article entitled "British spies betrayed to Russians and Chinese; Missions aborted to prevent spies being killed".[25] The article claimed that "Russia and China have cracked the top-secret cache of files stolen by the fugitive US whistle-blower Edward Snowden, forcing MI6 to pull agents out of live operations in hostile countries". Although the article was ridiculed by journalists familiar with the Snowden documents, among others, the claims were widely repeated by mainstream media outlets.[26]

22. National security was also used to justify the nine hour detention of David Miranda – the partner of journalist Glenn Greenwald, who led the Guardian's US reporting on Snowden's disclosures – under Schedule 7 of the Terrorism Act at Heathrow airport in August 2013. Under this measure – which is uniquely crafted for ports and airport transit zones before passengers have gone through passport control and entered Britain proper – individuals can be detained for nine hours with no right to legal representation and have their possessions confiscated for seven days. There is no requirement to arrest or charge a person with a terrorism related offence – indeed Miranda was never accused of being a terrorist or being associated with terrorists – and no protection is afforded to journalists or any sensitive material they may have in their possession. Miranda was carrying encrypted files, including 58,000 classified UK intelligence documents on an external hard drive, all of which were seized on the premise that their publication would cause "serious damage to UK national

[21] "Guardian faces fresh criticism over Edward Snowden revelations", Guardian, 10 November 2013, available at: http://www.theguardian.com/media/2013/nov/10/guardian-nsa-revelations-edward-snowden.
[22] "MPs grill Theresa May over spy chiefs' 'melodramatic soundbites' on NSA files", Guardian, 16 December 2013, available at: http://www.theguardian.com/politics/2013/dec/16/theresa-may-mps-spy-chiefs-nsa.
[23] "We have 'conclusive evidence' that Edward Snowden leaks hurt UK national security, say spy chiefs", Daily Mail, 11 April 2014, available at: http://www.dailymail.co.uk/news/article-2601977/We-conclusive-evidence-Edward-Snowden-leaks-hurt-UK-national-security-say-spy-chiefs.html.
[24] "'Traitor' Snowden endangered spies with NSA leaks, claim UK security chiefs", Russia Today, 18 March 2015, available at: http://rt.com/uk/241869-snowden-may-traitor-cost/.
[25] "British spies betrayed to Russians and Chinese", Sunday Times, 14 June 2015, available at: https://archive.is/BkuMM#selection-855.0-865.204.
[26] "Snowden files 'read by Russia and China': five questions for UK government", Guardian, 14 June 2015, available at: http://www.theguardian.com/us-news/2015/jun/14/snowden-files-read-by-russia-and-china-five-questions-for-uk-government.

security, and ultimately risk lives".[27] Miranda challenged the legality of his detention at the High Court, but in February 2014 three judges ruled that despite representing "an indirect interference with press freedom" his treatment was justified in the "very pressing" interests of national security. The judges refused to accept that the seized files were "journalistic material" and classified them instead as stolen data that was undeserving of any freedom of expression safeguards. They also rejected claims that Schedule 7 powers had been used to circumvent the legal requirement of judicial authorisation for the seizure of material from journalists (see para. 30-31).

III RELATED DEVELOPMENTS THAT HAVE WIDENED THE DEBATE ABOUT SURVEILLANCE

23. This section describes how the scope of the public debate in the UK that has taken place since the initial Snowden revelations has been widened by events, legal rulings and policy-making with a bearing on how surveillance is perceived or regulated. This provides the necessary background and context to the debates about surveillance reform discussed in subsequent sections.

Communications data retention for law enforcement purposes

24. Following the April 2014 ruling of the Court of Justice of the European Union invalidating the 2006 EU Data Retention Directive, the UK government fast-tracked domestic legislation to pre-empt any subsequent domestic legal challenge to the 2009 Data Retention (EC Directive) Regulations. Under those Regulations, Communications Service Providers (CSPs - internet service providers, mobile phone operators and telecommunications companies) were required to retain communications data from emails, phone calls and text messages for 12 months. As secondary legislation under the European Communities Act, the Regulations were vulnerable to judicial review, so the government introduced emergency legislation on 10 July 2014 in the form of the Data Retention and Investigatory Powers Bill. The 'emergency' allowed the Bill to be fast-tracked and it was agreed in less than four days of deliberations by the lower and upper Houses of Parliament.[28]

25. Confusingly, police and intelligence agency access to communications data retained under the Data Retention and Investigatory Powers Act (DRIPA) is governed by the Regulation of Investigatory Powers Act (RIPA). Applications to view this data must show that access is both "necessary" for one of the purposes defined by RIPA (this includes but is by no means limited to national security, the prevention and detection of crime, and public safety) and proportionate relative to potential intrusions of individual privacy. For both police and intelligence agencies these criteria are assessed internally by a "Designated Authorising Officer (a middle manager at an equivalent grade to Inspector or Superintendent in a police force)"; there is no *ex ante* external oversight from the judiciary or a surveillance court. This has resulted in a very high success rate in applications; a June 2015 report by the privacy campaign group Big Brother Watch showed that police grant themselves access to communications data 96% of the time. The report also revealed huge variation in rejection rates between different police forces – ranging from 28% to 0.1% - indicating that RIPA's

[27] "Miranda documents 'threaten UK security'", Channel 4 News, 30 August 2013, available at: http://www.channel4.com/news/miranda-documents-threaten-british-national-security.
[28] "Data Retention and Investigatory Powers Act 2014", Open Right Group, available at: https://wiki.openrightsgroup.org/wiki/Data_Retention_and_Investigatory_Powers_Act_2014.

guidelines are not being enforced uniformly.[29] In 2014, communications data was accessed approximately 460,000 times by the police and law enforcement agencies, and on approximately 50,500 occasions by intelligence agencies.[30] Nevertheless, the Interception of Communications Commissioner, Sir Anthony May, who provides retrospective oversight of authorisation procedures (see para. 56-58), claimed that his office "did not find significant institutional overuse of communications data powers by police forces and law enforcement agencies".

26. DRIPA is controversial because in key areas it effectively extends the surveillance powers set out in the Regulations it replaced. Although the government presented the proposals as simply providing a more robust statutory basis for data retention (Teresa May called it a "narrow and limited" Bill), the Act widens the definition of "telecommunications service" to include services such as webmail and TOR, and provides for warrants for interception and communications data acquisition requests to be made to companies not based in the UK. DRIPA has been widely criticised by civil society organisations (para. 86-89) and academics (para. 96-97), who object to the manner in which the Act was adopted and argue that it is incompatible with the ruling by the ECJ. The Act is the subject of an ongoing Judicial Review (see para. 73).

27. The short debate around DRIPA paved the way for future reforms to UK surveillance law, with the government replicating provisions made by the US government in the wake of the Snowden revelations. The Act includes a 'sunset clause' under which it will expire at the end of 2016, and made provision for a recently completed Review of Communications Data and Interception Powers (para. 62-68). An Independent Civil Liberties Oversight Board, evidently inspired by the Privacy and Civil Liberties Oversight Board established by US Presidential decree, will oversee aspects of UK surveillance policy; and a Special Envoy on intelligence and law enforcement data sharing was appointed to represent the UK government in negotiations with CSPs, the US and other international partners (see para. 59-61).

The 'Snoopers' charter'

28. The Communications Data Bill, nicknamed the "Snoopers' charter" by privacy campaigners, was draft legislation that would have required UK CSPs to significantly expand the range of communications data they hold on their users. In addition to data already retained under DRIPA and its predecessor, CSPs would have been required, *inter alia*, to log internet browsing history (weblogs), social media interactions and online gaming for 12 months under a blanket regime. The Bill was presented by the government as necessary to enable UK security agencies to "keep pace" with changing digital technology and new online communication services (Skype, Twitter, Facebook, WhatsApp, and Snapchat etc.). The government argued that communications data from these sources must be collected and retained for the purpose of investigating terrorism and serious crime.

29. The case for increased retention of communications data was first made in 2008 by the then Labour government's "Interception Modernisation Programme". The programme was shelved in the run up to the 2010 general election but was swiftly revived by the new Conservative-Liberal Democrat coalition government under a different name: the

[29] "Police Access to Communications Data", Big Brother Watch, May 2015, available at: https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/05/Big-Brother-Watch-Report-Police-Communications-Data1.pdf.
[30] "Interception of Communications Commissioner's Report 2014", 12 March 2015, available at: http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20%28Web%29.pdf.

"Communications Capabilities Development Programme". The draft Communications Data Bill was duly announced in May 2012,[31] but under pressure from their supporters and members of parliament, the Liberal Democrats withdrew their support for the Bill the following year, available at: Following the Conservative Party's electoral victory in May 2015, Home Secretary Theresa May signalled her intent to reintroduce the legislation. Plans for a new Investigatory Powers Bill were duly included in the May 2015 Queen's Speech, which set out the legislative programme of the new government.

Surveillance and the protection of journalists' sources

30. The Snowden revelations have led journalists to question their ability to protect the confidentiality of their sources, including potential whistleblowers, from overbroad government surveillance powers. Whilst express approval from a judge is needed before police can seize documents from a journalist, under RIPA's aforementioned provisions it is senior police officers who approve police applications for access to journalists' phone and email records.

31. In February 2015, the Interception of Communications Commissioner (see para. 56-58), Sir Anthony May, reported that over a three year period 19 police forces had put in more than 600 applications to view journalists' phone records in order to identify their sources. In the face of heavy criticism, the government introduced emergency guidelines on the protection of journalists' communications (see para. 83).

Surveillance and legal privilege

32. Like journalists, lawyers have voiced concerns about the protection of confidential attorney-client communications in the face of mass surveillance. These concerns would ultimately be put before the IPT after the Snowden revelations alerted lawyers representing two men, who were suing the UK government for its role in their rendition from China to Libya, to the fact that state surveillance may have compromised their right to a fair trial. In 2004, Abdul-Hakim Belhaj and Sami al Saadi, both Libyan nationals and known Gaddafi dissidents, were kidnapped in China along with their families and rendered to Libya where they were imprisoned for six years and subjected to repeated torture. Libyan security service documents released after the fall of the Gaddafi regime revealed the central role that the UK government had played in their rendition.

33. In October 2014, following the Snowden revelations, the human rights organisations Reprieve and Amnesty International filed a claim with the Investigatory Powers Tribunal alleging that the security services had been intercepting their private communications with both Al-Saadi and Abdul-Hakim. The government admitted that the intelligence services have policies regarding the interception of private calls between lawyers and their clients, but would not go into greater detail because doing so might "be damaging to public interest or prejudicial to national security."[32]

34. In February 2015, the government conceded that in the absence of clearly defined legal safeguards, the UK intelligence agencies' monitoring of conversations between lawyers and their clients had been unlawful. It has now published an updated draft code of practice to

[31] Draft Communications Data Bill 2012, June 2012, available at: http://www.parliament.uk/draft-communications-bill/.
[32] "Abdul-Hakim Belhaj and Fatima Boudcha", Reprieve, available at: http://www.reprieve.org.uk/case-study/abdul-hakim-belhaj/.

meet these requirements and ensure that interceptions can continue on a legal footing (see para. 83).

35. In April 2015, the Investigatory Powers Tribunal ordered GCHQ, Britain's national security surveillance agency, to destroy the legally privileged communications it had unlawfully collected from Al-Saadi. This was the first time the IPT had ever ordered the intelligence services to relinquish surveillance material obtained unlawfully.[33]

Surveillance of activists and non-governmental organisations

36. RIPA was amended following revelations regarding the infiltration of protest groups by undercover police officers to "increase the amount of independent supervision and assessment of undercover operations".[34] Many of the officers involved in what is known as the "spycops" scandal have been shown to have acted as agent provocateurs and some had long-lasting sexual relationships with members of the groups they were sent to spy on, in at least two cases fathering children. The Office of Surveillance Commissioners – which oversees the use of covert surveillance by public authorities - must now be notified at the outset of operations and give prior approval for all undercover deployments which last longer than 12 months. Within police forces, all deployments of undercover officers must be authorised by an assistant chief constable, while those lasting more than 12 months must be approved by a chief constable.

37. In June 2015, the Investigatory Powers Tribunal confirmed that GCHQ had been monitoring at least two international NGOs: the Egyptian Initiative for Personal Rights and South Africa's Legal Resources Centre. The tribunal would not reveal why the groups were being monitored and, crucially, did not find the surveillance to be illegal, in effect accepting the right of UK intelligence agencies to monitor human rights organisations across the world (see para. 84).

Surveillance and extra-judicial killing

38. Documents leaked by Snowden have called into question the role of UK intelligence agencies in facilitating covert US drone strikes outside recognised war zones. A 'top secret' GCHQ memo revealed how a joint US, UK and Australian programme codenamed "Overhead" supported a drone strike in Yemen in 2012. Jemima Stratford QC, who provided legal advice to the UK All Party Parliamentary Group on Drones in 2014 arguing that the arrangements for the collection and exchange of intelligence material were unlawful,[35] said of the "Overhead documents": "In our view, if GCHQ transferred data to the NSA in the knowledge that it would or might be used for targeting drone strikes that transfer is probably unlawful".[36] Further, "These documents underline why greater transparency as to UK official policies would help to ensure legality from a domestic and international law perspective".

[33] "Secretive court orders GCHQ to destroy stolen documents", Reprieve, 29 April 2015, available at: http://www.reprieve.org.uk/press/secretive-court-orders-gchq-to-destroy-stolen-documents/.
[34] "Legislation strengthens independent oversight of undercover police operations", 31 October 2013, available at: https://www.gov.uk/government/news/legislation-strengthens-independent-oversight-of-undercover-police-operations.
[35] "Huge swath of GCHQ mass surveillance is illegal, says top lawyer", Guardian, 28 January 2014, available at: http://www.theguardian.com/uk-news/2014/jan/28/gchq-mass-surveillance-spying-law-lawyer.
[36] "GCHQ documents raise fresh questions over UK complicity in US drone strikes", Guardian, 24 June 2014, available at: http://www.theguardian.com/uk-news/2015/jun/24/gchq-documents-raise-fresh-questions-over-uk-complicity-in-us-drone-strikes.

39. The government maintains it's strict "neither confirm nor deny" policy in relation to targeted killings, a stance rejected by Conservative MP David Davis. He said "It's no good the government hiding behind its standard security line that they never comment on security matters. The phrase extra-judicial killing is a euphemism. What we are talking about here is murder…It is important the government makes plain: what are the limitations it puts on the use of its intelligence, and under what statutes and on whose approval this information is shared?" A former head of GCHQ, David Omand, joined Davis in signing a letter calling on the government to reveal its guidelines on intelligence-sharing for the purpose of covert drone strikes.

Counter-terrorism investigations and access to communications data

40. An inquiry conducted by the Intelligence and Security Committee into the murder of British soldier Lee Rigby by two men, Michael Adebolajo and Michael Adebowale, in Woolwich, southeast London, in May 2013, was highly critical of the operational practices of foreign communications service providers. The committee suggested that had UK intelligence agencies been able to monitor an online exchange between Adebowale and foreign extremists prior to Rigby's murder, the attack *might* have been prevented. But the company on whose system the exchange took place (which was widely reported to be Facebook), "does not regard themselves as under any obligation to ensure that they identify such threats, or to report them to the authorities. We find this unacceptable: however unintentionally, they are providing a safe haven for terrorists".[37] None of the major US CSPs, the committee found, proactively monitor user content, nor do they feel obliged to grant access when presented with UK warrants obtained under RIPA. "They appear to accept no responsibility for the services they provide. This is of very serious concern: the capability of the Agencies to access the communications of their targets is essential to their ability to detect and prevent terrorist threats in the UK."

41. In the wake of Snowden's disclosures, increasing numbers of international communications service providers have opted to introduce or enhance security and encryption protocols to protect the privacy of their customers. The government responded by intimating that it will legislate to prevent communications being rendered inaccessible to the security services. Although the efficacy and associated security provided by the various forms of encryption is debated, a growing number of popular CSPs now claim that the measures they have introduced leave them powerless to decipher their customers' communications, which means that even were they inclined to grant intelligence agencies access to their content, they would now be unable to do so.

42. In January 2015, Prime Minister David Cameron gave a speech in which he argued that the security services must always have the capability to read peoples' communications and stated that the government would introduce "legislation that makes sure we do not allow terrorists safe space to communicate with each other". Although he did not articulate how this could be achieved in practice, the only conceivable way to achieve this outcome would be to demand 'backdoors' for security agencies, or to attempt to ban the use of certain forms of encryption and the applications and services which utilise it.

[37] ISC Press Release, November 2014, available at: http://isc.independent.gov.uk/files/20141125_ISC_Press_Release_Woolwich.pdf.

IV INQUIRIES AND REVIEWS BY THE UK PARLIAMENT AND OTHER SIGNIFICANT ACTORS

43. This section describes the establishment and where possible the outcomes of the reviews of various elements of surveillance policy and practice that have taken place in the UK parliament, been commissioned by the UK government or arisen out of statutory requirement. While these reports have increasingly demanded reform of UK surveillance legislation, they have, without exception, identified the core problem as not enough oversight, rather than too much surveillance.

Parliamentary Committees

44. The Intelligence and Security Committee (ISC) is a statutory committee of Parliament established in 1994 to oversee the expenditure, administration and policies of UK intelligence agencies. Its mandate was expanded in 2013 (prior to the Snowden revelations) to include their operational activities, military intelligence, the security and intelligence activities of the government, and counter-terrorism in the Home Office. Its nine members – appointed by parliament after nomination by the prime minister – are subject to the Official Secrets Act 1989 and allowed to access highly classified material. The committee takes evidence from government ministers and senior intelligence agency officials almost entirely in secret. Its credibility, impartiality and effectiveness have long been questioned. The director of the human rights NGO Liberty, Shami Chakrabarti, commented: "The ISC has repeatedly shown itself as a simple mouthpiece for the spooks - so clueless and ineffective that it's only thanks to Edward Snowden that it had the slightest clue of the agencies' antics."[38]

45. On 7 June 2013, following the initial Snowden revelations that GCHQ had received data via the Prism programme, the ISC announced that it "will be receiving a full report from GCHQ very shortly and will decide what further action needs to be taken as soon as it receives that information."[39] On 17 July 2013, the Committee announced that they had analysed detailed evidence from GCHQ and concluded that the organisation's use of Prism to access the content of private communications "has not circumvented or attempted to circumvent UK law".[40] The ISC found that in each case where GCHQ sought information from the US, "a warrant for interception, signed by a Minister, was already in place". While strictly true in the legal sense, the implication that such surveillance is targeted masks the fact that vast quantities of data is shared to allow the 'targeting'.

46. Overall the ISC's 'investigation' was extremely limited in scope, looking only at instances where GCHQ *requested* data from the US. It failed to consider the legality of the NSA supplying UK intelligence agencies with the personal data of British citizens and individuals living in the UK. Nor did it consider what happened when US agencies offered information to their UK counterparts voluntarily. The investigation was focussed only on instances where the content of communications had been intercepted, not the vast amounts of communication data that had been collected by Prism. GCHQ's own internet surveillance programme, Tempora, was not even mentioned. The investigation did, however, conclude that it was necessary for the ISC to evaluate whether the UK's legislative framework for regulating access to private communications was fit for purpose in the digital age.

---

[38] "Intelligence report branded 'clueless' by Liberty director", ITV News, 12 March 2015, available at: http://www.itv.com/news/update/2015-03-12/intelligence-report-branded-clueless-by-liberty-director/.
[39] ISC Press Release, 7 June 2013, available at: http://isc.independent.gov.uk/news-archive/7june2013.
[40] "Statement by the ISC regarding GCHQ's alleged access to the US PRISM programme", 17 July 2013, available at: http://isc.independent.gov.uk/files/20130717_ISC_statement_GCHQ.pdf.

47. On 17 October 2013, the ISC announced that due to widespread concern over the extent of UK intelligence agencies' surveillance capabilities, the committee's inquiry into the suitability of the UK's legislative framework would be broadened to consider whether an appropriate balance was currently being struck between "our individual right to privacy and our collective right to security."[41] To ensure that "the full range of opinions expressed on these topics" were considered, the inquiry invited written evidence more broadly, including from the public, in addition to classified evidence heard in secret.

48. In May 2014 the Home Affairs Select Committee published a report on UK counter-terrorism capabilities. Following the Snowden revelations, the Committee had held a dedicated hearing on their implications for national security (supra para. 20). Keith Vaz MP called the disclosures and "embarrassing indictment" of the UK's system of democratic scrutiny.[42] The report called for reform of the system of oversight of MI5, MI6 and GCHQ, finding that "the latitude afforded to congressional committees [in the USA] to examine intelligence matters by the executive is perhaps the key difference between the US system and the UK system where the Government consistently refuses to allow committees other than the ISC to ask questions on the work of the security and intelligence agencies. Given that a number of important issues have been raised and debated as part of the work of the Judiciary Committees, it is perhaps telling that the debate has been more charged in the US where more representatives are able to scrutinise the work of such agencies."[43]

49. On 12 March 2015, following an 18 month inquiry, the ISC published its second report, "Privacy and Security: A modern and transparent legal framework".[44] Its two principle findings were that: (i) "The UK's intelligence and security agencies do not seek to circumvent the law"; and (ii) "The legal framework is unnecessarily complicated and – crucially – lacks transparency". The "key recommendation" stemming from the inquiry was "that the current legal framework be replaced by a new Act of Parliament governing the intelligence and security Agencies. This must clearly set out the intrusive powers available to the Agencies, the purposes for which they may use them, and the authorisation required before they may do so".

50. The ISC's report provided the first official acknowledgement of GCHQ's "bulk interception capability", but claimed that while the practice "may involve large numbers of emails, it does not equate to blanket surveillance, nor does it equate to indiscriminate surveillance" due to the targeting and filtering systems in place. The ISC reasoned that because GCHQ has access only to a small percentage of the global internet structure its practices cannot be considered "blanket interception", but ignored the fact that greater access is de facto achieved through close cooperation with the intelligence agencies of other countries. These findings were strongly contested by human rights groups and privacy campaigners (see para. 87). Crucially,

[41] ISC Press Release, 17 October 2013, available at: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20131017_ISC_statement_privacy_and_security_inquiry.pdf.
[42] "MPs: Snowden files are 'embarrassing indictment' of British spying oversight", Guardian, 9 May 2014, available at: http://www.theguardian.com/uk-news/2014/may/09/edward-snowden-mps-commons-report-spying.
[43] "Home Affairs Committee - Seventeenth Report: Counter-terrorism", 30 April 2014, available at: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23103.html.
[44] "Privacy and Security: A modern and transparent legal framework", ISC, 12 March 2015, available at: http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf.

the ISC report made no recommendations on how data sharing with the US and other countries should be regulated.

51. Speaking on behalf of the Committee, then Labour MP Hazel Blears said: "What we've found is that the way in which the agencies use the capabilities they have is authorised, lawful, necessary and proportionate. But what we've also found is there is a degree of confusion and lack of transparency about the way in which this is authorised in our legal system." This lack of transparency, the report warns, "could be misconstrued as providing the Agencies with a 'blank cheque' to carry out whatever activities they deem necessary."[45]

52. Significantly, the report acknowledged the lack of statutory oversight for "bulk personal datasets". The government responded by releasing a statement granting "statutory powers of oversight" to the intelligence services commissioner, Sir Mark Waller (see para. 57).

The Royal United Services Institute

53. In March 2014, having failed to convince his Conservative coalition partners of the need for a broad inquiry to review the accountability structure of UK intelligence agencies, Nick Clegg, then Deputy Prime Minister and leader of the Liberal Democrats, commissioned an independent review of internet surveillance practices and their control and oversight by the Royal United Services Institute.

54. The RUSI review is modelled on that commissioned by US President Barack Obama in January 2014 on 'big data' and privacy. Clegg wrote in the Guardian that "the quality of the debate in the US provides an unflattering contrast to the muted debate this side of the Atlantic".[46] The key terms of reference of the review are: (i) Advise on the legality, effectiveness and privacy implications of UK surveillance programmes, particularly as revealed by the Snowden leaks; (ii) Examine potential reforms to current surveillance practices, including additional protections against the misuse of personal data, and alternatives to the collection and retention of bulk data; (iii) Make an assessment of how law-enforcement and intelligence capabilities can be maintained in the face of technological change, while respecting principles of proportionality, necessity and privacy.[47]

55. RUSI is a registered charity that traces its history back to 1829. Although independent from government, it has been described by David Wearing of the University of London as "very much a creature of the British state and military establishment, without which it would neither have been created nor would it exist in recognisable form today".[48] The twelve members of RUSI's Independent Surveillance Review Panel are former heads of GCHQ, MI5, MI6 and the Metropolitan Police's intelligence directorate; professors of journalism, law, computer science, history and philosophy; the founder of online travel agency Lastminute.com and a former director of Nominet, the UK domain registry.[49] RUSI described

[45] Supra.
[46] "Edward Snowden's revelations made it clear: security oversight must be fit for the internet age", Guardian, 3 March 2014, available at: http://www.theguardian.com/commentisfree/2014/mar/03/nick-clegg-snowden-security-oversight-internet-age.
[47] "Independent Surveillance Review Panel Announced", RUSI News, 12 June 2014, available at: https://www.rusi.org/news/ref:N5399836649AAC/#.VZPI1EaHAeW.
[48] "Why is the BBC presenting RUSI as objective analysts of the Middle East?", Open Democracy, 12 June 2015, available at: https://www.opendemocracy.net/ourbeeb/david-wearing/why-is-bbc-presenting-rusi-as-objective-analysts-of-middle-east.
[49] Supra, note 47.

the panel as representing "all the major interests surrounding surveillance issues; industry, governmental policy-making, security, scholarship, civil society concerns and parliamentary considerations". There have no public proceedings or calls for evidence and no apparent outreach to civil society organisations or human rights groups. The panel's report is expected to be published in mid-July 2015.

Interception of Communications Commissioner

56. The Interception of Communications Commissioner (ICC), Sir Anthony May, is responsible for reviewing how intelligence agencies, police forces and public authorities use RIPA to intercept communications and to acquire and disclose communications data. The ICC is responsible for ensuring that these bodies act in accordance with their legal responsibilities under the Act and reviews the role of the Home Secretary in issuing interception warrants. The exercise of these functions is documented in bi-annual report (until the adoption of DRIPA, the reports were produced annually). Giving evidence to the House of Commons Home Affairs Committee, May described RIPA as "an extremely difficult act of parliament to get your mind round".[50]

57. The ICC is one of three commissioners appointed under RIPA to provide independent oversight and scrutiny of surveillance functions. Oversight of the intelligence agencies (except interception practices) is carried out by the Intelligence Services Commissioner, Sir Mark Waller. And oversight of covert surveillance in public and private places, the use of covert human intelligence sources and property interference comes from the Chief Surveillance Commissioner, Sir Christopher Rose. Each commissioner is a retired High Court or Appeal Court judge appointed by the Prime Minister, to whom they report. In addition, the Surveillance Camera Commissioner, Tony Porter, reviews the operation of covert CCTV systems against a code of practice. Reports by the ISC and the government's Independent Reviewer of Terrorism Legislation have both recommended reform of the commissioner system; the former advocated greater staffing and resourcing and an increased role for each commissioner, the latter called for the three posts to be merged under a new body, the Independent Surveillance and Intelligence Commission (see para. 65).

58. In his annual report for 2013, published in April 2014, the ICC directly addressed concerns that surveillance powers were being misused, and mounted a robust defence of surveillance policy and practice within his purview, stating that: "Public authorities do not misuse their powers under RIPA Part I to engage in random mass intrusion into the private affairs of law abiding UK citizens. It would be comprehensively unlawful if they did". May further stated that he was "quite clear that any member of the public who does not associate with potential terrorists or serious criminals or individuals who are potentially involved in actions which could raise national security issues for the UK can be assured that none of the interception agencies which I inspect has the slightest interest in examining their emails, their phone or postal communications or their use of the internet, and they do not do so to any extent which could reasonably be regarded as significant". May also stated that "British intelligence agencies do not circumvent domestic oversight regimes by receiving from US agencies intercept material about British citizens which could not lawfully be acquired by

[50] "Law on GCHQ is complex, says watchdog", Guardian, 11 February 2014 , available at: http://www.theguardian.com/uk-news/2014/feb/11/gchq-number-personal-data-intercepts-law-too-many-official.

intercept in the UK".[51] It is important to stress, however, that the ICC's mandate is limited to those activities that fall under the scope of RIPA, with many of GCHQ's communications data gathering operations outside his remit. As the Commissioner himself acknowledged, "I am not appointed or authorised to oversee all of the activities of the intelligence agencies, only those specified in Section 57(2) of RIPA".[52] Thus despite the apparently robust defence of the kinds of surveillance revealed by Snowden, May's report makes no mention of programmes like Tempora or Prism, or the links between intelligence agencies and communications service providers. His assertion that the intelligence agencies have no interest whatsoever in the communications of 'ordinary' members of the British public, or indeed those of ordinary citizens anywhere else, is in my view therefore open to question.

Special Envoy on intelligence and law enforcement data sharing

59. Sir Nigel Scheinwald, formerly a British ambassador to Washington, has operated as the Prime Minister's Special Envoy on intelligence and law enforcement data sharing since September 2014.[53] He was asked to report on alternatives to mandatory telecommunications data retention as provided for by the Data Retention Investigatory Powers Act (supra para. 24-27) and envisaged by the so-called "Snooper's Charter" (supra para. 28-29).

60. Scheinwald's report was completed in the spring of 2015, but has been classified "Top Secret" by the Cabinet Office and withheld from the public. The government claims that there is no requirement to publish the report because the Special Envoy "is not undertaking a public review". The conclusions were leaked to the Guardian newspaper, and following complaints by privacy campaigners that the government was trying to stifle debate about surveillance reform,[54] a two page summary was published.[55]

61. The summary notes the importance of "limited and proportionate access to private communications" and the impact that encryption and legal reforms are having on intelligence and law enforcement agencies "capability to access data in a readable format". The summary sets out four "longer term proposals": (i) improve "government-to-government cooperation" and "data sharing between like-minded countries"; (ii) reforming the US-UK Mutual Legal Assistance Treaty to enable faster and more responsive processing of requests for data; (iii) developing a new international framework that will allow UK agencies to "gain access to content in serious crime and counter-terrorism cases through direct requests to [US CSPs]"; (iv) improving transparency around the number and nature of our requests to overseas and domestic Communication Service Providers make it faster and easier. Scheinwald's proposals represent a credible alternative to achieving the stated

[51] "2013 Annual Report of the Interception of Communications Commissioner", April 2014, available at: http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf.
[52] "Sir Anthony May's response to the Article published in the Independent", ICC Office, 13 March 14, available at: http://www.iocco-uk.info/sections.asp?sectionID=8&chapter=4&type=top.
[53] "Sir Nigel Sheinwald appointed Special Envoy on intelligence and law enforcement data sharing", Cabinet Office, 19 September 2014, available at: https://www.gov.uk/government/news/sir-nigel-sheinwald-appointed-special-envoy-on-intelligence-and-law-enforcement-data-sharing.
[54] "Secret report urges treaty forcing US web firms' cooperation in data sharing". Guardian, 2 June 2015, available at: http://www.theguardian.com/world/2015/jun/02/web-firms-data-sharing-secret-treaty.
[55] "Summary of the Work of the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing – Sir Nigel Sheinwald", available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/438326/Special_Envoy_work_summary_final_for_CO_website.pdf.

objectives of the "Snooper's Charter" which, when it was last proposed in the form of the Communications Data Bill in 2012, contained provisions to compel UK communications service providers to collect personal data passing through their networks originating from US companies that refused to cooperate on a voluntary basis with UK access requests.

Independent Reviewer of Terrorism Legislation

62. In July 2014, in accordance with the Data Retention and Investigatory Powers Act, the Independent Reviewer of Terrorism Legislation, David Anderson, was instructed to lead a wide-ranging review of the investigatory capabilities and powers required by law enforcement and intelligence agencies, and the regulatory framework within which those capabilities and powers should be exercised.

63. The Independent Reviewer is tasked with overseeing the operation of the UK's Laws on terrorism and informing public and political debate through regular reports made to parliament. The role's statutory functions were expanded by the Counter-Terrorism and Security Act 2015 to allow for the review of recent terrorism legislation, although the Independent Reviewer is unable review powers that were not expressly designed for counter-terrorism purposes. The Act also created a Privacy and Civil Liberties Board (PCLB), inspired by its equivalent US body, the Privacy and Civil Liberties Oversight Board. However, "the name of the new Board remains a poor guide to its actual functions" according to Anderson, who added that: "In a well-ordered world, such matters would have been the subject of pre-legislative consultation and considered action".[56] The PCLB was originally intended to replace the Independent Reviewer, but will now work under Anderson's direction and control.

64. Anderson's report, "A Question of Trust", was published on 11 June 2015.[57] It was intended to "inform the public and political debate on these matters, which at its worst can be polarised, intemperate and characterised by technical misunderstandings"; to "satisfy the majority who broadly accept current levels of investigatory activity and supervision"; and "to help build trust among sceptics both in the UK and abroad". Echoing the principal findings of the earlier ISC report (supra para. 49), Anderson concluded that "The current law is fragmented, obscure, under constant challenge and variable in the protections that it affords the innocent… It is time for a clean slate". The report makes 124 separate recommendations to this effect.

65. Eight of the recommendations are particularly significant in terms of their potential impact on surveillance reform. (i) A new law should be drafted that is "comprehensive in its scope and comprehensible to people across the world". It would replace the current multitude of confusing legislation; a state of affairs that is "undemocratic, unnecessary and - in the long run - intolerable". (ii) DRIPA powers requiring UK CSPs to retain communications data for law enforcement and security purposes (supra para. 24-27) should continue to exist, subject to legal restraints. (iii) Bulk data collection capabilities should be retained "but used only subject to strict additional safeguards" and to the addition of a new and lesser power to collect only communications data in bulk. (iv) The case has not yet been made for the 'Snoopers' Charter' (supra para. 28-29). Legislation requiring CSPs to retain weblogs should

[56] "Independent Review and the PCLB", Independent Reviewer of Terrorism Legislation, 31 January 2015, available at: https://terrorismlegislationreviewer.independent.gov.uk/independent-review-and-the-pclb/.
[57] "A Question of Trust – Report of the Investigatory Powers Review", Independent Reviewer of Terrorism Legislation, 11 June 2015, available at: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

only be introduced once "a detailed operational case can be made out and a rigorous assessment has been conducted of the lawfulness, likely effectiveness, intrusiveness and cost" of requiring such data to be retained. (v) The distinction between 'internal' and 'external' communications is outdated in the context of internet communications and should be abandoned. (vi) Judicial authorisation should be required for all interception warrants (by judicial commissioners); the role of ministers should be limited to saying some warrants are required in the interests of national security. (vii) Judicial authorisation should be required if the police want to obtain communications data from lawyers, journalists, and others who receive information in confidence (see para. 82-84). (viii) The three existing Commissioners that deal with surveillance (supra para. 57) should be replaced by a new Independent Surveillance and Intelligence Commission; a "well-resourced and outward-facing regulator" composed of retired judges that would take over the judicial authorisation of all warrants, authorise contentious and sensitive requests for communications data, and issue guidance.

66. Anderson declared himself largely satisfied as to the legitimacy of 'mass surveillance' as practiced through bulk interceptions, although he qualified this position by stressing that "It is not my function to offer a legal assessment, particularly in a case that is under consideration by a senior court" (a reference to the cases pending at the European Court of Human Rights, see para. 70-72). However, he also stated that GCHQ case studies "leave me in not the slightest doubt that bulk interception, as it is currently practised, has a valuable role to play in protecting national security. It does not of course follow that it is necessarily proportionate, which is for the courts to decide."

67. Anderson's most radical proposal, that government ministers should lose their power to approve interception warrants to judicial authorities, has already been rebuffed by the Prime Minister, whose spokeswoman emphasised that law enforcement and intelligence agencies need to be able "to respond quickly and effectively to threats of national security or serious crime".[58]

68. Home Secretary Theresa May responded to the report by promising an overhaul of investigatory powers legislation. She said that Anderson's report, together with the ISC report and the forthcoming RUSI review, provided a firm basis for legislation. May told parliament that she would publish a draft surveillance bill in the autumn of 2015 and expected the new legislation to be adopted before the end of 2016.

V JUDICIAL REVIEW AND SURVEILLANCE REFORM

69. This section provides an overview of the judicial review of surveillance powers sought by non-governmental organisations and other critical stakeholders concerned with fundamental rights and democratic controls. In doing so it provides an overview of the substantive positions taken by these organisations with respect to the exercise and democratic control of surveillance. In a climate of muted debate about surveillance, these cases have kept the issue in the public sphere and provided a counter-narrative to the government's spin and obfuscation. This section also provides a summary of the legislative and non-legislative reforms to surveillance law and practice that have resulted from the cases brought by NGOs.

Mass surveillance and the right to privacy

[58] "UK intelligence agencies should keep mass surveillance powers, report says", Guardian, 11 June 2015, available at: http://www.theguardian.com/world/2015/jun/11/uk-intelligence-agencies-should-keep-mass-surveillance-powers-report-gchq.

70. In July 2014, Amnesty International, Liberty, Privacy International, the American Civil Liberties Union and several other non-UK based groups lodged a legal challenge to the Tempora programme at the Investigatory Powers Tribunal, arguing that "mass surveillance" undertaken by the programme is unlawful, and that by obtaining information from the NSA, UK intelligence agencies have sidestepped protections afforded by the UK legal system. As noted above (supra para. 8-9), the government still refuses to confirm or deny that the Tempora programme exists.

71. In December 2014, the IPT ruled that the UK's legal regime governing mass surveillance was lawful in principle. The tribunal's decision was based on previously secret internal policies governing data sharing with the US that the government was forced to disclose during the case (albeit in closed hearings, with descriptions provided to the claimants). However, this brought into question whether the government's surveillance regime complied with the law prior to these disclosures being made, and in a second ruling in February 2015 the tribunal found that intelligence sharing between the United States and the United Kingdom was unlawful prior to December 2014. This was the first time the IPT had ruled against the intelligence and security services in its 15 year history.

72. The claimants have now made a joint application to the European Court of Human Rights to appeal the IPT's initial December 2014 ruling. Amnesty claims: "The government has managed to bluff their way out of this, retreating into closed hearings, and constantly playing the 'national security' card. The tribunal has accepted that approach. We have had to painstakingly drag out every detail we could from an aggressively resistant government… The government's entire defence has amounted to 'trust us' and now the tribunal has said the same."[59] The appeal is likely to be heard together with a separate challenge to the UK's 'mass surveillance' programmes brought by Big Brother Watch, Open Rights Group, English PEN and the German activist Constanze Kurz, which is currently being fast-tracked by the ECHR. These groups elected to bypass the IPT because it "is a creature of the very statutory regime which has failed and would not offer an effective remedy".[60]

73. Judgment is currently pending in the High Court's judicial review of the 2014 Data Retention and Investigatory Powers Act (supra para. 24-27), which took place in June 2015 following a complaint brought by MPs David Davis and Tom Watson represented by Liberty. The case has broadly the same substantive merits as the successful challenge to the EU Data Retention Directive at the ECJ. The MPs' lawyer said: "Their concern is that this legislation doesn't contain the necessary minimum safeguards to protect against the risk of arbitrary, disproportionate or abusive retention and use of personal data, and for that reason it breaches the fundamental right to privacy". Davis has been scornful of the manner in which the Act was "driven through the House of Commons with ridiculous and unnecessary haste to meet a completely artificial emergency… As a result members of parliament had no opportunity to either research it, consider it or debate it properly and the aim of this legal action is to make the government give the House the opportunity to do what it should have been allowed in the first place. Proper, considered and effective law making".[61]

---

[59] "UK court decision on government mass surveillance: 'Trust us' isn't enough", Amnesty, 5 December 2014, available at: https://www.amnesty.org/en/latest/news/2014/12/uk-court-decision-government-mass-surveillance-trust-us-isnt-enough/.

[60] "Privacy not Prism", available at: https://www.privacynotprism.org.uk/.

[61] "Two MPs to sue government over data law 'stitch-up'", Channel 4 News, 22 July 2014, available at: http://www.channel4.com/news/data-drip-law-surveillence-tom-watson-david-davis-legal-sue.

74. In June 2015, GCHQ's use of "bulk personal datasets" was challenged for the first time when Privacy International filed a legal complaint at the Investigatory Powers Tribunal. The US's equivalent domestic powers (under section 215 of the PATRIOT Act) had been curtailed just days earlier with the passing of the USA Freedom Act. Privacy International acted in response to the Intelligence and Security Committee's report of March 2015 which revealed that no proper legal regime is in place for the acquisition and subsequent use of datasets. Access does not require judicial or ministerial approval, and there are no legal penalties for misuse. Privacy International argues: "Secretly ordering companies to hand over their records in bulk, to be data-mined at will, without independent sign off or oversight, is a loophole in the law the size of a double-decker bus. The use of these databases, some volunteered, some stolen, some obtained by bribery or coercion, has already been abused, and will continue to be, until the practice is overhauled, and proper protections put in place".[62]

'Hacking'

75. Privacy International has also filed two separate complaints to the IPT challenging GCHQ hacking, or "computer network exploitation". They and other NGOs are concerned that hacking is more invasive than the other forms of surveillance and or data-gathering revealed by Snowden because it provides access to potentially vast amounts of highly personal data that could not otherwise be obtained. The interception of communications can only reveal what an individual has chosen to communicate; hacking allows the intelligence agencies to view material that might never have been voluntarily disclosed. More invasive still, by covertly taking control of a computer or mobile device, GCHQ can activate applications such as a camera, microphone or global positioning system to generate content without its owner's knowledge or consent. Hacking is also at the heart of intelligence agencies efforts to break or by-pass encryption protocols, a practice that Tim Berners-Lee, inventor of the World Wide Web and founding director of the World Wide Web Foundation, called "appalling and foolish" because it is likely to "benefit criminal hacker gangs and hostile states". Berners-Lee has stressed that he is "very sympathetic to attempts to increase security against organised crime, but you have to distinguish yourself from the criminal".[63]

76. Privacy International's first complaint, filed in May 2014, challenges the agency's "extensive and intrusive" hacking of personal computers and devices. Snowden's leaked documents revealed that GCHQ, often in partnership with the NSA, has been "infecting potentially millions of computer and mobile devices around the world with malicious software that gives them the ability to sweep up reams of content, switch on users' microphones or cameras, listen to their phone calls and track their locations."

77. Privacy International's second complaint was filed in July 2014 in conjunction with seven international communications service providers – Riseup (US), GreenNet (UK), Greenhost (Netherlands), Mango (Zimbabwe), Jinbonet (Korea), May First/People Link (US), and the Chaos Computer Club (Germany) – against GCHQ's exploitation of CSP network infrastructure to conduct mass and intrusive surveillance. The widespread nature of these attacks was documented in a series of articles in Der Spiegel and The Intercept. They revealed that GCHQ had a range of network exploitation and intrusion capabilities that had been used to target a number of CSPs, including the Belgian telecommunications giant

[62] Press Release, Privacy International, 8 June 2014, available at: https://www.privacyinternational.org/?q=node/594.

[63] "Tim Berners-Lee: encryption cracking by spy agencies 'appalling and foolish'", Guardian, 6 November 2013, available at: http://www.theguardian.com/world/2013/nov/06/tim-berners-lee-encryption-spy-agencies.

Belgacom and internet exchange points run by three German companies, Stellar, Cetel and IABG.

78. In each complaint, Privacy International contends that GCHQ's activities are unlawful both under the Computer Misuse Act 1990, which criminalises hacking, and under Articles 8 and 10 of the European Convention of Human Rights, which stipulate that any interference of privacy and freedom of expression must be a governed by a clear legal framework to guard against abuse of power and arbitrary use. Since GCHQ had not divulged the legal basis for its hacking activities, Privacy International assumed that the justification under domestic law was a warrant issued under section 5 of the Intelligence Services Act 1994, which permits "entry on or interference with property or with wireless telegraphy" in certain circumstances, and in cases of hacking outside the UK a warrant under section 7 of the Act which purports to immunise from criminal liability "any act done outside the British Islands, if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section...".[64]

79. In May 2015, the day before Privacy International's second complaint was due to be heard at the IPT, the government revealed in its legal filings that the Computer Misuse Act had been rewritten to exempt law enforcement and intelligence agencies from criminal liability for hacking. The law had been amended through a seemingly minor "clarifying amendment" of the Serious Crimes Bill, which received royal assent on 3 March 2015 and come into effect on 3 May 2015. Privacy International responded: "The explanatory notes that accompanied the act make no reference to the true impact of the change. It appears no regulators, commissioners responsible for overseeing the intelligence agencies, the Information Commissioner's Office, industry, NGOs or the public were notified or consulted about the proposed legislative changes. There was no published Privacy Impact Assessment. Only the Ministry of Justice, Crown Prosecution Service, Scotland Office, Northern Ireland Office, GCHQ, Police and National Crime Agency were consulted as stakeholders. There was no public debate."[65]

80. The government had already reacted to claims that GCHQ's hacking regime breached ECHR requirements for clear formal legal guidelines by publishing a draft Equipment Interference Code of Practice in February 2015.[66] The draft code, which was relied on heavily by the government in its open response to the two IPT cases, purportedly mirrors internal GCHQ guidance. It was subject to a six week public consultation, feedback from which is currently being considered. The government would not disclose GCHQ's earlier versions of the code to Privacy International or reveal when it was first dated, citing national security considerations.[67] The draft code publicises the circumstances and procedures surrounding computer network exploitation for the first time, confirming that intelligence agencies have broad powers to hack into personal computers and phones and exploit communications networks anywhere in the world, even if the target is not a perceived threat to national security or suspected of having committed a criminal offence. The government has been

[64] Statement of Grounds, available at: https://www.privacyinternational.org/sites/default/files/Final%20Grounds%20-%20GCHQ%20attacking%20providers_0.pdf.
[65] Press Release, Privacy International, 15 May 2014, available at: https://www.privacyinternational.org/?q=node/584.
[66] "Draft Equipment Interference Code of Practice", 6 February 2005, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401863/Draft_Equipment_Interference_Code_of_Practice.pdf.
[67] Supra, note 65.

criticised by prominent academics for attempting to legislate on highly invasive practices with minimal democratic scrutiny through a code of practice, rather than primary legislation (see para. 96-97).[68]

Freedom of Information and intelligence sharing arrangements

81. The European Court of Human Rights has also admitted a September 2014 legal challenge brought by Privacy International of GCHQ's blanket exemption from the UK's Freedom of Information Act. Privacy International contends that intelligence agencies should not be allowed to keep data sharing arrangements with other countries secret, and that it is in the public interest for GCHQ to be required to "publish documents which stipulate how surveillance is shared with and obtained by Five Eyes partners, including the NSA".[69]

Protection of journalists, lawyers and NGOs

82. The ECHR is fast tracking a case brought by the Bureau of Investigative Journalism in September 2014 over the lack of protection afforded to journalists and their sources by UK legislation from mass surveillance and interception programmes. The court has been asked to rule on the adequacy of legal safeguards in RIPA against unjustified surveillance by all relevant authorities. Gavin Millar QC, who has been instructed by TIBJ's lawyers, asserted that "Police misuse covert RIPA powers to get journalists' metadata – and so identify sources – routinely now. This circumvents the rights of a journalist to protect a source and to a hearing before a judge before any order is made to disclose such information. The sheer volume of data being harvested by GCHQ under RIPA means that confidential journalistic material is also being covertly accessed and analysed by security and intelligence all the time. Again sources are being identified – but on a much larger scale. Yet there is no word in RIPA or the government's code of practice under it about these key journalistic rights. The UK simply flouts the Convention."[70]

83. As noted above, following earlier complaints to the Intelligence Powers Tribunal by Amnesty and Reprieve concerning the surveillance of lawyer-client communications (supra para. 30-31), the government published draft 'codes of practice' for state surveillance of confidential communications between lawyers, journalists, MPs and members of the public. Kat Craig, legal director of Reprieve, described the proposals as having "failed dismally to strike the balance between security and privacy.[71] At best they expose the government's failure to grasp the risks of modern day surveillance powers. At worst, they suggest a more sinister reluctance to submit to the rule of law. Of course surveillance plays a crucial role in our nation's safety, but this can be equally well achieved with proper safeguards in place – something which these proposals clearly fail to provide."

---

[68] "Snowden slams UK government attempts to secretly pass legislation allowing GCHQ to 'hack anybody's computer'", computing.co.uk, 02 Jun 2015, available at: http://www.computing.co.uk/ctg/news/2411261/snowden-slams-uk-government-attempts-to-secretly-pass-legislation-allowing-gchq-to-hack-anybodys-computer.

[69] "Privacy International v. United Kingdom" , available at: https://www.privacyinternational.org/?q=node/83.

[70] "Bureau files ECHR case challenging UK government over surveillance of journalists' communications", The Bureau of Investigative Journalism, 14 September 2014, available at: https://www.thebureauinvestigates.com/2014/09/14/bureau-files-echr-case-challenging-uk-government-over-surveillance-of-journalists-communications/.

[71] "Government's new lawyer-snooping guidance "fails dismally"", Reprieve, 20 March 2015, available at: http://www.reprieve.org.uk/press/governments-new-lawyer-snooping-guidance-fails-dismally-reprieve/.

84. In June 2015, the IPT found procedural errors in GCHQ's monitoring of two international NGOs. Significantly the tribunal did not find the surveillance itself to be unlawful; rather it was GCHQ's failure to follow its own secret internal rules that broke the law.[72] In the case of the Egyptian Initiative for Personal Rights, communications were found to have been "retained for materially longer than permitted" by GCHQ guidelines. And in the case of South Africa's Legal Resources Centre, procedure for selection of communications for examination was "in error not followed". The two groups were part of a large consortium of NGOs taking action against the government. The IPT found that GCHQ had no case to answer to the other claimants – including Amnesty International, Liberty and Privacy International – and therefore did not reveal whether or not they had been monitored. Due to national security concerns the tribunal also refused to reveal why it was deemed necessary and proportionate for GCHQ to spy on the Egyptian Initiative for Personal Rights and South Africa's Legal Resources Centre. In essence, however, the IPT accepted that UK intelligence agencies have a legal right to monitor foreign civil liberties NGOs.

VI CIVIL SOCIETY CAMPAIGNS

85. This section explains the public positions taken by key actors from 'civil society' with regard to the impact and reform of surveillance policy and practice. It includes positions taken by NGOs, academics, and professional bodies.

'Don't Spy On Us'

86. The 'Don't Spy On Us' campaign – a coalition of UK and international civil liberties groups including Liberty, ARTICLE19, Big Brother Watch, English PEN, Open Rights Group and Privacy International – was formed in February 2014 to provide concerted opposition to "unfettered mass state surveillance".[73]

87. The campaign and its members have been strongly critical of the reports by Parliament's Intelligence and Security Committee, in particular its finding that GCHQ does not engage in 'mass surveillance' (supra para. 44-52). "How else can the filtering of billions of communications and the searching through of those communications with tens of thousands of selectors be described?", it asked.[74] "No amount of technical and legal jargon can obscure the fact that this is a parliamentary committee, in a democratic country, telling its citizens that they are living in a surveillance state and that all is well", countered Privacy International.[75]

88. Conversely, the NGOs were broadly welcoming of the review conducted by the Independent Reviewer of Terrorism Legislation (supra para. 62-68) and the "frank manner in which he confronts the truths revealed by the Snowden documents about surveillance overreach – a

[72] "GCHQ intercepts communications of human rights groups", Liberty, 22 June 2015, available at: https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/gchq-intercepts-communications-human-rights-groups.
[73] "Don't Spy On Us", available at: https://www.dontspyonus.org.uk/.
[74] "UK Parliament's Intelligence Committee says reform needed after Snowden revelations", Don't Spy On Us, March 2015, available at: https://www.dontspyonus.org.uk/blog/2015/03/12/uk-parliaments-intelligence-committee-says-reform-needed-after-snowden-revelations/.
[75] Press Release, Privacy International, 12 March 2015, available at: https://privacyinternational.org/?q=node/505.

first for any official report or review in the UK since the revelations began two years ago."[76] Liberty suggested that his "thoughtful report... could be the beginning of re-building public trust in surveillance conducted with respect for privacy, democracy and the law."[77] They expressed disappointment, however, that in recommending a move away from arbitrary distinctions between 'internal' and 'external' communications, Anderson did not speak out against discriminatory privacy protections under which British citizens and residents enjoy more rights than foreigners: "His recommendations enshrine the government's position that mass surveillance of foreigners is an acceptable activity of a democratic state, and improve protections for Britons while entrenching privacy intrusions for everyone else."[78]

89. The Don't Spy On Us campaign makes 13 specific recommendations for surveillance reform in the UK: (i) RIPA and DRIPA must be repealed and replaced by new comprehensive surveillance legislation; (ii) All surveillance decisions (including the interception of communications and access to communications data) must be subject to prior judicial authorisation; (iii) The interception of communications must always be targeted and specific rather than mass and indiscriminate; (iv) Communications data should be afforded the same protection as the content of communications. The retention of metadata should also be targeted and specific; (v) Surveillance should only be carried out for purposes that are more precisely and narrowly defined than at present; (vi) The government should cease breaking encryption standards and undermining internet security. Such activity should be explicitly prohibited by legislation; (vii) International arrangements governing the collection and sharing of the results of surveillance must be made public, subject to parliamentary and judicial oversight and should allow individuals to foresee when they are likely to be subject to surveillance. This requirement should be set out in legislation; (viii) The government should publish aggregate information on the number of surveillance authorisation requests approved and rejected in order to increase transparency; (ix) Adequate remedies should be available for the unlawful access to communications data and the unauthorised use of other surveillance techniques; (x) The Investigatory Powers Tribunal should adopt a more open and fair procedure. This should include: hearings; public hearings, unless the government demonstrates that secrecy is required in the particular case; evidence should be disclosed and judgments and reasons published unless the government demonstrates that secrecy is necessary; special advocates should be appointed; decisions should be subject to appeal; (xi) The Intelligence and Security Committee should be reformed so that it is: answerable directly to Parliament; empowered to take decisions on reporting and publication; and appropriately funded and staffed. It should have strengthened powers to compel the production of information and witnesses. The chair should be a member of the largest opposition party and the Commons members should be elected not appointed by the Whips; (xii) The Intelligence Services Commissioner and the Interception of Communications Commissioner should be properly resourced, report to Parliament and review a far larger number of requests for data; (xiii) Intercept evidence should be admissible in criminal court proceedings.[79]

---

[76] Press Release, Privacy International, 11 June 2015, available at: https://www.privacyinternational.org/?q=node/595.

[77] "Undemocratic, unnecessary and – in the long run – intolerable": Government reviewer condemns Britain's snooping laws", Liberty, 11 June 2015, available at: https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/%E2%80%9Cundemocratic-unnecessary-and-%E2%80%93-long-run-%E2%80%93-intolerable%E2%80%9D.

[78] Press Release, Privacy International, 11 June 2015, available at: https://www.privacyinternational.org/?q=node/596.

[79] "Reforming surveillance in the UK", Don't Spy On Us, September 2014, available at: https://www.dontspyonus.org.uk/assets/files/pdfs/reports/DSOU_Reforming_surveillance.pdf.

"Open up the Five Eyes"

90. Following the Snowden revelations, London-based Privacy International launched the "Eyes Wide Open" campaign with the aim of prying open the Five Eyes arrangement and bringing it under the rule of law.[80] The campaign stresses the level of integration between the UK and US intelligence agencies, citing intelligence officials who have stated that the level of co-operation under the UKUSA agreement is so complete that "it becomes very difficult to know who is doing what [...] it's just organizational mess." Another senior member of the UK intelligence community is quoted as saying "When you get a GCHQ pass it gives you access to the NSA too. You can walk into the NSA and find GCHQ staff holding senior management positions, and vice versa."

91. The launch of the "Eyes Wide Open" campaign was accompanied by the publication of a report, according to which "The patchwork of secret spying programmes and intelligence sharing agreements implemented by parties to the Five Eyes arrangement constitutes an integrated global surveillance arrangement that now covers the majority of the world's communications."[81] The report calls for an appreciation of "interference-based jurisdiction" that reflects "the way the global communications infrastructure is built" and "enables the right to privacy of communications can be exercised globally."

Professional bodies and Trade Unions

92. Professional associations representing lawyers and journalists have been strongly critical of the surveillance practices revealed by Snowden, voicing repeated concerns about their on their members.

93. "Whistleblower Edward Snowden has called on professionals, including lawyers, to upgrade security following surveillance revelations", the UK Law Society told its members in the aftermath of the initial disclosures,[82] while backing calls for a "public debate on surveillance issues."[83] The Law Society's President explained: "I will be writing to other professional bodies so we can discuss the impact spying is now having on our members' confidential communication with clients or patients. I will also be writing to relevant academics, civil liberties groups, lawyers and other experts both nationally and internationally, to invite them to collaborate with us in addressing wider issues on surveillance and the rule of law." A Law Society press release issued in response to the 'emergency' data retention legislation adopted in 2014 noted: "It is difficult to overstate our concern about the possible effects of the Data Retention and Investigatory Powers law that was rushed through parliament by the government this week". The Law Society called for reforms "to simplify and clarify a complex and confusing legal framework to ensure that it protects human rights."[84]

94. The National Union of Journalists (NUJ) has been even more vocal in its criticism of surveillance powers and support for whistleblowers, journalists and the protection of their

[80] "Eyes Wide Open", Privacy International, available at: https://www.privacyinternational.org/?q=node/42.
[81] "Eyes Wide Open: Special Report", Privacy International, 26 November 2013, available at: https://www.privacyinternational.org/sites/default/files/Eyes%20Wide%20Open%20v1.pdf.
[82] "Cyber security", Law Society, available at: http://www.lawsociety.org.uk/support-services/practice-management/cyber-security/.
[83] "Law Society backs public debate on surveillance issues", 18 July 2014, available at: http://www.theguardian.com/world/2014/jul/18/law-society-debate-surveillance.
[84] "Stark warning on emergency surveillance legislation", Law Society, 10 July 2014, available at: http://www.lawsociety.org.uk/news/press-releases/stark-warning-on-emergency-surveillance-legislation/.

sources, issuing numerous statements, hosting conferences and offering free training to its members on privacy and information security.[85] In April 2014, the NUJ passed a motion calling for a commission to be set up to look at new legislation to protect individuals and organisations against unnecessary state surveillance.[86]

95. The NUJ also tabled a motions that was adopted at the 2013 Trades Union Congress (the UK's federation of trade unions) with overwhelming support. The motion stated that "Congress is particularly concerned about the unprecedented industrial scale of NSA and GCHQ secret data trawling and internet surveillance of tens of millions of citizens, British among them, revealed by former US NSA contractor Edward Snowden. Congress believes that the protection of privacy, beyond the necessity of providing a legal shield for whistleblowers, is of clear public interest, especially in the realm of freedom of information."[87]

Academia

96. In May 2015, a group of 38 UK-based academics published an open letter to MPs urging the new government "to ensure that any changes in the law, and especially any expansions of power, are fully and transparently vetted by Parliament, and open to consultation from the public and all relevant stakeholders."[88] Some of the letter's signatories had also signed an international declaration entitled "Academics Against Mass Surveillance" published in January 2014.[89] Some had also written to the government in July 2014 to argue that the then Data Retention and Investigatory Powers Bill should be subject to full and rigorous parliamentary scrutiny because it represented "a serious expansion of the British surveillance state". They objected in particular to the Home Secretary's characterisation of the legislation as merely a re-affirmation of the UK's pre-existing data retention regime, when in fact it substantially expanded investigatory powers (supra para. 26).

97. The May 2015 letter notes that this casual approach to due process has continued, with surveillance powers being "presented in a way seemingly designed to stifle robust democratic consideration". The signatories criticise the manner in which the government has attempted to introduce rules on hacking through a code of practice rather than primary legislation, and the exemption granted to the police and intelligence services for criminal liability for hacking through a "clarifying amendment" contained in the Serious Crimes Act 2015. Anticipating that the new parliament's legislative agenda will include the revival of the Communications Data Bill and a review of RIPA, the letter calls on the government to expand surveillance powers only through primary legislation and with due consideration of privacy rights enshrined in the European Convention of Human Rights. "The Government should not be permitted to surreptitiously change the law whenever it so desires, especially where such changes put our privacy and security at risk".

---

[85] NUJ website, available at: https://www.nuj.org.uk/site-search/?&keywords=snowden&p=2.
[86] "DM2014: Orwell's worst dream", NUJ, 12 April 2014,available at: https://www.nuj.org.uk/news/dm2014-orwells-worst-dream/.
[87] "Congress backs campaigns on workplace bullying, mass surveillance and to scrap the lobbying bill", NUJ, 13 September 2013, available at: https://www.nuj.org.uk/news/congress-backs-campaigns-on-workplace-bullying-mass/.
[88] "Ensuring the Rule of Law and the democratic process is respected as UK surveillance law is revised", Open letter to UK Parliament, 27 May 2015, available at: http://www.technollama.co.uk/open-letter-to-uk-parliament-about-surveillance.
[89] "Hundreds of academics protest against mass surveillance", Wired, 3 January 2014, available at: http://www.wired.co.uk/news/archive/2014-01/03/academics-against-mass-surveillance.

98. The concerns related to hacking echoed an open letter dated September 2013 from the University of Bristol Cryptography Group, which stated: "By weakening cryptographic standards, in as yet undisclosed ways, and by inserting weaknesses into products which we all rely on to secure critical infrastructure, we believe that the [intelligence] agencies have been acting against the interests of the public that they are meant to serve. We find it shocking that agencies of both the US and UK governments now stand accused of undermining the systems which protect us. By weakening all our security so that they can listen in to the communications of our enemies, they also weaken our security against our potential enemies. We call on the relevant parties to reveal what systems have been weakened so that they can be repaired, and to create a proper system of oversight with well-defined public rules that clearly forbid weakening the security of civilian systems and infrastructures."[90]

99. It is also notable that in October 2014, the UK Economic and Social Research Council awarded a grant to Cardiff University's School of Journalism, Media and Cultural Studies to fund an 18 month project "Digital citizenship and surveillance society: UK state-media-citizen relations after the Snowden Leaks" to explore "the nature, opportunities and challenges of digital citizenship in light of governmental surveillance measures".[91] The project's preliminary findings highlight public concern over the "lack of transparency on the level of state surveillance in the UK… people are acutely aware of surveillance happening online, be it by the state, corporations, employers or peers… but also feel powerless to do much about it. This relative resignation to the realities of mass surveillance in the UK arguably stands in contrast to developments we are witnessing in Germany and the US two years on from the Snowden leaks".[92]

100. Finally, there has been substantial and ongoing debate among UK legal scholars about the legitimacy and compatibility of the surveillance practices revealed by Snowden with the UK Human Rights Act and corresponding international laws.[93] However it is fair to say that for the most part debates about issues such as the extra-territorial applicability of the UK's human rights obligations vis-à-vis signals intelligence collection have failed to capture the public's imagination.

VII THE SIGNIFICANCE OF THIS INFORMATION FOR GERMANY

101. In spite of government intransigence, parliamentary deference to the intelligence agencies, and a preference on the part of many in prominent media positions for questioning the integrity and motives of Snowden (and the journalists with which whom he worked), the public debate in the UK has been characterised by a gradual but fundamental shift toward the universal recognition that wholesale reform of UK surveillance legislation is now both necessary and desirable. As the government's Independent Reviewer of Terrorism

[90] "Open Letter From UK Security Researchers", Bristol Cryptography Blog, available at: http://bristolcrypto.blogspot.co.uk/2013/09/open-letter-from-uk-security-researchers.html.
[91] "Digital Citizenship and Surveillance Society", DCSS project, available at: http://www.dcssproject.net/.
[92] "Edward Snowden's lawyer among prestigious line-up of privacy campaigners, scholars, journalists and tech experts in Cardiff for major surveillance event", Cardiff University, 18 June 2015, available at: http://www.cardiff.ac.uk/news/view/113535-edward-snowdens-lawyer-among-prestigious-line-up-of-privacy-campaigners,-scholars,-journalists-and-tech-experts-in-cardiff-for-major-surveillance-event.
[93] See for example, "UK Human Rights Blog" (http://ukhumanrightsblog.com/), "Blog of the European Journal of International Law" (http://www.ejiltalk.org/tag/surveillance/), and "UK Constitutional Law Association" (http://ukconstitutionallaw.org/).

Legislation observes: "The opportunity now exists to take a system characterised by confusion, suspicion and incessant legal challenge, and transform it into a world-class framework for the regulation of strong and vital powers".[94]

102. However, whereas all stakeholders now recognise the need for reform, some reforms are clearly more likely to materialise than others. Consolidation and simplification of the primary legislation governing the activities of the intelligence agencies and surveillance powers, in particular the Regulation of Investigatory Powers Act 2000 and the innumerable legislative acts, codes of practice and oversight mechanisms that govern its implementation is inevitable (the government has already promised a comprehensive legislative package). It is also likely that the proposals will build on the moves toward increased *ex-poste* administrative and parliamentary oversight, and statistical reporting of basic qualitative data about surveillance. But it remains to be seen if the UK government will be willing to countenance – or if parliament will demand – anything approaching the level of modest reform already witnessed to in the USA.

103. Notwithstanding the potential impact of future judgments in cases before the UK and European courts, the government and those it has called upon for advice on surveillance reform have declared themselves largely satisfied with the level of surveillance that the intelligence agencies conduct, signalling that significant restriction of their current powers and capabilities is unlikely. In this context, the human rights community views *ex-ante* judicial authorisation of surveillance activities as the only credible means of ensuring that those powers are only exercised when it is necessary and proportionate to do so. However, the government has also signalled its intention to maintain the UK's position as the only Five Eyes country with no form of judicial pre-authorisation for internet and telecommunications surveillance.

104. Crucially for Germany and indeed the rest of the world is the abject lack of debate that has taken place in respect to the need or otherwise to restrict the UK's foreign intelligence gathering operations. The UK intelligence agencies involvement in spying on the governments of its partners in the EU, for example, has barely raised a murmur of dissent beyond the pages of the newspapers that carried the revelations. This is partly because UK civil society organisations have sought to keep the spotlight on 'mass surveillance' of the general population, but also reflects the suggestion that people everywhere are generally much more tolerant of government surveillance of foreigners.[95]

105. Another crucial yet largely unaddressed element of the post-Snowden debate is the offensive 'hacking' activities of the UK intelligence agencies. These are significant in the context of steps taken by many companies and private citizens around the world to protect their communications by using privacy-enhancing technologies or platforms. The UK intelligence agencies currently enjoy almost limitless powers to 'hack' public networks and private computers with impunity, and the government has recently provided them with significant funding to enhance these capabilities. It can be expected therefore that the government will seek to enshrine and mount a robust defence of these powers in forthcoming debates around legislative reform.

[94] Supra, note 57.

[95] Chris Chambers, "The psychology of mass government surveillance: How do the public respond and is it changing our behaviour?", Guardian, 18 March 2015, available at: http://www.ejiltalk.org/the-power-of-citizenship-bias/.

106. There has also been an abject lack of critical debate about the merits or otherwise of the UK's 'special relationship' with the USA, its other "Five Eyes" partners, and those countries including Germany who have partnered the Five Eyes in the various configurations of 'Five Eyes plus'. In my view this represents a systematic failure on the part of national debates to tackle the central proposition and implications of Snowden's claim that the Five Eyes should be understood as a "supra-national intelligence organisation that doesn't answer to the known laws of its own countries". In the absence of such debate, there is every chance that current transnational intelligence sharing arrangements will be largely unaffected by the UK's pending reforms.

107. In this context and by way of conclusion it may be stressed, as I and others have noted elsewhere, that unless other major European powers raise the bar substantially in respect to the restriction of surveillance and the democratic control of their own intelligence agencies, particularly with regard to foreign intelligence collection, it is simply not credible for others to expect the same of the UK.[96] As the UK's Special Envoy on intelligence and law enforcement data sharing has recently advised, constructing a new international framework that enables cross-border access to communications data in strictly limited and appropriately supervised circumstances, is the only tangible alternative to the international status quo.

[96] Ian Brown, Morton H. Halperin, Ben Hayes, Ben Scott and Mathias Vermeulen, "Towards Multilateral Standards for Surveillance Reform", Oxford Internet Institute Discussion Paper, January 2015, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2551164.