Surveillance for the masses

Burkhard Schafer

Surveillance for the masses: the political and legal landscape of the UK Investigatory Powers Bill

In March 2016, the UK Government put the Investigatory Powers Bill before Parliament. The new law, if enacted, will considerably increase the powers of law enforcement and security services regarding mass data retention, mass surveillance and mass hacking. This raises considerable concerns not just about the content of the Bill and its impact on privacy, but also about the method of its enactment and the ever diminishing parliamentary and judicial scrutiny of surveillance legislation in the UK.

1 The Investigatory Powers Bill

On March the 15th 2016, the Investigatory Powers Bill (IPB) passed its second reading at the House of Commons, the lower chamber of the British Parliament. The Bill, once enacted, will substantially increase the powers of UK intelligence and law enforcement agencies for targeted interception of communications, the bulk collection of communications data, and mass interception of communications. This marks for the time being the culmination of a process that formally started in November 2015, when the draft Bill was first presented to Parliament. To understand the full significance of the new law however, we will have to go further back in history, tracing its ancestry back to the Data Retention and Investigatory Powers Act of 2014 and the unsuccessful attempt in 2013 to enact the draft Communications Data Bill.

The Bill, in its present form, is a massive 229 pages long.[1] In addition, the government published a 67 pages "explanatory note" that not only provides for the policy rationale, but also an explanation and interpretation of key terms and concepts. Even more importantly, the Bill comes with six Codes of Practice, totalling over 400 pages in length, which describe in more detail the implementation of the new powers, and any safeguards and restrictions that the agencies ought to observe. It is, obviously, impossible to give a detailed account of all the provisions in the IPB here. More detailed analysis and comprehensive resources can be found inter alia at the Media Policy Project of the LSE[2] or the website of the Independent Reviewer for Terrorism Legislation.[3] Instead, we will try to put the Bill in its historical and political context for German readers, to enable them to see the proposal as a continuation of a theme of surveillance in Britain that sets it more and more apart from continental Europe. The paper will conclude with some thoughts on the issues that the IPB may face now that the UK has decided to leave the EU.

2 From RIPA to IPB, a history of UK surveillance legislation

While the IPB was submitted to Parliament by a conservative (Tory) government, Labour, as the main opposition party, has been generally muted in its criticism of the proposed legislation. To explain this and to understand the political process that shapes the current discussion of the Bill, we have to go back to at least 2000, when the then Labour government enacted the Regulation of Investigatory Powers Act RIPA. RIPA is currently the main legal framework governing surveillance and similar "data driven" investigative activities, including the interception of communications. Just as the present Bill, it was justified at the time by a perceived need to update police powers in line with technological change, such as the growth of electronic communication, strong encryption and the increasing pervasiveness of large data sets such as CCTV records. From its inception, the Act was criticised by privacy advocates and academics for the wide range of powers it granted, and the weak system of oversight that it established for them.[4]

RIPA complemented and underpinned considerable investment under the Labour government in surveillance technology and surveillance capabilities. It is best understood not just in the context of the growth of the Internet and the investigation of cybercrime, but the general growth of "evidence-led policing" and technology-enabled surveillance. At the time RIPA was enacted, the UK became e.g. the country with the world's most extensive use of CCTV by public authorities for the

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf

[2] http://blogs.lse.ac.uk/mediapolicyproject/2016/01/05/some-things-old-some-things-new-a-clause-by-clause-review-of-the-draft-investigatory-powers-bill-investigatory-powers-research-group/

[3] https://terrorismlegislationreviewer.independent.gov.uk/investigatory-powers-bill-the-major-issues/

[4] See e.g. Akdeniz, Y., Taylor, N. and Walker, C. (2001). "Regulation of Investigatory Powers Act 2000: Bigbrother. gov. uk: State surveillance in the age of information and rights, Criminal Law Review 73-90; Reid, A.S. and Ryder, N. (2001). For Whose Eyes Only? A Critique of the United Kingdom's Regulation of Investigatory Powers Act 2000. *Information & Communications Technology Law*, *10*(2), 179-201.

purpose of crime prevention. RIPA not only provided the legal framework for the police to make use of these new surveillance capabilities. As one of its most problematic aspects, it also granted considerable surveillance powers and data access rights to a plethora of public agencies, from local councils to the environmental agency, the gambling commission or the food standards authority. While intended to be used only in the prevention and investigation of serious crime and terrorism, it soon transpired that these authorities also used their newfound powers for much less pressing social issues such as dog fouling or benefit fraud. This was often driven by one of the most problematic provisions in the Act, which allows surveillance not just for protection against national security threats and crime, but also for the prevention of "economic harm".

The combination of far-reaching surveillance powers under RIPA, a weak and fragmented supervisory system and the significant investment in and proliferation of surveillance technology caused the Information Commissioner Richard Thomas to warn that "Britain was sleepwalking into a surveillance state".[5] In 2009, the House of Lords report „Surveillance: Citizens and the State" painted, in over 300 pages, a dire picture of the increasing imbalance between privacy protection and state surveillance. Despite these criticisms from both inside Parliament and independent officials, the government stayed its course, marking also a power shift away from parliament and parliamentary scrutiny to a stronger executive. Britain's "unwritten constitution" and its reliance on soft conventions make it susceptible to this type of power shift.

However, by 2009 and in the run-up to a general election, a marked shift in public perception had occurred. Widespread misuse of RIPA powers had made civil liberties an election issue for the British public. An unlikely alliance between libertarian leaning members of the Conservative party and the Liberal Democrats, traditionally the party of civil liberties ensured that commitment to law reform became part of the election manifesto of both opposition parties. The election, highly unusual for Britain, did not give an overall majority to any party, forcing the Conservatives into a coalition government with the Lib Dems – the first coalition government in living memory. With both parties committed to stronger protection of civil liberties and privacy, some commentators hoped for a sustained shift in the UK's approach to police powers, while others, including the author in an earlier DuD contribution, remained sceptical.[6]

The new government did indeed initially honour its manifesto pledges. The Identity Documents Act 2010 (c. 40) repealed the Identity Cards Act 2006 and in effect abolished the Identity Card Scheme, pushed by Labour against the objections of privacy advocates. The Protection of Freedoms Act (2012) reigned in DNA collection and CCTV surveillance.

However, initial improvements soon gave way to a more surveillance friendly approach. The Interception Modernisation Programme, a programme from the dying days of the Labour government to extend the capabilities for interception and storage of communications data similar to the NSA Call Database, [7] was revived as "Communications Capabilities Development Programme" (CCDP).[8] Its aim is to develop the capacity to log the meta-data of every telephone call, email and text message between UK residents extending the reach beyond conventional telecommunications media to social networking platforms such as Twitter.[9] In parallel to providing significant funding for this project, the Home Office introduced in 2012 the Draft Communications Data Bill as the enabling law for the programme. Dubbed by opposition and the media as a "snooper's charta", it would have required ISPs and mobile phone companies to keep records of Internet browsing activity, email correspondence, voice calls, Internet gaming, and mobile phone messaging services for 12 months. The Bill also contained provisions for data queries and data matching across different data sources, the "filter provisions" (similar to a "Rasterfahndung") for a wide range of circumstances and reasons, including protection of "the economic wellbeing of the UK" in the absence of any specific threat. In 2013, the LibDems withdrew their support for the Bill, leaving the government without a majority and risking defeat in the House of Common. For the time being, the Bill was withdrawn – while work on the CCDP continued apace.

In the same year, the Snowden disclosures about PRISM revealed the extent of mass surveillance by the British security services, in particular GCHQ, and the extend of data sharing with the US security agencies. The legal basis for these activities remained questionable. The Snowden files showed inter alia that despite assurances given to Parliament, and arguably in violation of RIPA, UK security services had used raw data collected by the US services without a warrant signed by a minister of state. They also showed that GCHQ routinely collected bulk communication meta-data. It is at least questionable if RIPA authorizes the collection of bulk data. For all its shortcomings, RIPA is still based on the ideal of targeted surveillance of specified individuals who are under suspicion of having committed or are about to commit specific crimes. The activities taken by the security services were possibly based on a legally dubious "extensive" interpretation of the term "person" in the RIPA provisions – so at least the conclusion reached in a review by the Independent Reviewer of Terrorism Legislation, who remained highly critical of this interpretation.[10] Alternatively, the mere collection of mass data might be deemed to fall short of "surveillance" for the purpose of RIPA, which would mean that as long as the data is not used or accessed, no warrant is required. This was the answer of the Investigatory Powers Tribunal, the judicial body charged under RIPA with adjudicating complaints against surveillance by public bodies. In response to complaints raised post-Snowden by Liberty, the Human Rights NGO, it ruled in late 2014 that bulk collection of data was not "surveillance" as long as the data was not seen by a human eye, and did therefore not raise legal issues. The tribunal did however confirm as an obiter that untargeted mass surveillance remained in principle impermis-

[5] For a detailed discussion of this report see Schafer, B. (2009). Schlafwandelnd in den Überwachungsstaat?. *Datenschutz und Datensicherheit-DuD*, *33*(8), 483-489.

[6] Schafer, B. (2011). All changed, changed utterly?. *Datenschutz und Datensicherheit-DuD*, *35*(9), 634-638.

[7] See on the programme Walker, C. (2009). Data retention in the UK: Pragmatic and proportionate, or a step too far?. *Computer Law & Security Review*, *25*(4), 325-334.

[8] See Edwards, L., Rauhofer, J., and Yar, M. (2013). Recent developments in UK cybercrime law. *Handbook of Internet Crime*, 413-436.

[9] Brown, I. (2012). Government access to private-sector data in the United Kingdom. *International Data Privacy Law*, ips018.

[10] David Anderson, A question of Trust, p. 96 https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

sible under that Act.[11] In a later decision, it ruled furthermore that the warrantless data sharing between US and UK agencies had indeed been unlawful – but that paradoxically, the Snowden revelations had remedied this by creating the necessary "public knowledge" of the activity.[12]

These decisions indicated that the regulatory and enforcement regime of RIPA was insufficient to control security services – either because they were able to ignore with impunity the law due to the weakness and fragmentation of the supervisory agencies, or because the law was so restrictively worded that even highly problematic activities fell outside its remit.

While the Lib Dems had been the traditional party of civil liberties, they found themselves in government with an increasingly surveillance friendly senior partner just at a time when the Snowden revelations laid bare the degree of surveillance in the UK – increasing the pressure from their own voter base to be more assertive and push back more aggressively against state intrusion into private communication.

Finally, in August 2014, the European Court of Justice ruled in *Digital Rights Ireland Ltd* and *Seitlinger and others*, that the EU Data Retention Directive was incompatible with the rights to privacy and data protection under the Charter of Fundamental Rights, and thus void. Since the Directive had been the basis of the data retention duties under RIPA, the decision also invalidated significant parts of the British legal surveillance framework. Rather than abandoning bulk surveillance though, the Home Office pushed for a different solution. In their reading, the safeguards provided by RIPA made the UK surveillance regime immune from challenges under the Charter. To maintain data gathering capacities and to continue data retention by UK ISPs, emergency legislation was introduced that restored the legal data retention duties that the voided Directive had mandated. The Data Retention and Investigatory Powers Act 2014 (DRIP) was passed after minimal parliamentary scrutiny on 14 July 2014 with cross-party support. Conservatives, Lib Dems and Labour overwhelmingly for the Bill, only the representatives of nationalist parties from devolved parts of the UK (The Scottish National Party, the Welsh Plaid Cymru and the Northern Irish SDLP) voted against.

This indicated one of the constitutional law problems with this Bill, and the regulation of communication interception in the UK in general. Under e.g the Scotland Act 1998 that established the devolved Scottish Parliament, Scotland has sole legislative competence in all issues not explicitly reserved to the UK government in Westminster under Schedule 5 of the Act. National defence, the security services and communication interception are such reserved matters under sec B8 of Schedule 5. However, policing and crime investigation are not. RIPA therefore has a UK and a Scottish (Irish, Welsh) dimension, and the devolved parliaments and assemblies will be charged with implementing parts of it. Despite this, there was no involvement with or consultation of the leaders of the devolved parliaments, and as the UK does not have an equivalent to the German Bundesrat or the US Senate, there is also no legislative body that directly involves the devolved regions in the legislative process at the federal, Westminster level. The anomalies that this setup creates became visible in the discussion on DRIP.

Constitutional concerns, however, also marred the very process chosen to enact DRIP. Submitting the law as emergency legislation meant minimal parliamentary scrutiny, restricting debate to just four days. Several commentators pointed out that the crisis was largely manufactured by the Home Office which apparently had not followed the progression of the *Digital Rights Ireland* case at court, and even after the verdict was given initially delayed its response by several months. Shami Chakrabarti, the then director of Liberty, spoke about "an essay crisis rather than a national crisis", aptly comparing the Home Office to a student who waited too long before doing their assessment.[13] Parliamentarians from all parties echoed this concern. However, in the absence of a written constitution and a Supreme Court that can enforce procedural rules, in the UK context this is seen as primarily a political, not a legal question.

The government justified its stance by claiming that DRIP only reaffirmed powers already granted under RIPA, which had been before Parliament. This however not only ignored the changing landscape created by the CJE decision, it was also based on a problematic reading of RIPA powers. On the face of it, DRIP extended existing interception powers under RIPA in at least two ways: it extended the territorial scope of the provisions significantly, by granting new powers to force overseas companies to store communication data and assist UK authorities with interception capacities. Secondly, it extended the scope of companies that could be compelled to assist the police beyond traditional communication providers to social media platforms and other online service providers. According to the government, these powers had been implicit in the wording of RIPA, but neither a plain text reading of the law, nor a consultation of the traveaux preparatoires or the Parliamentary discussion supports that interpretation.[14] There were a number of concessions made for unhappy backbenchers amongst the main parties. Most importantly, the Act came with a sunset clause of one year, which at the time was seen as a small victory for privacy advocates, but would prove to be a double edged sword. The Reviewer of Terrorism Legislation was tasked with providing the above-cited comprehensive report on surveillance legislation in the UK. Finally, a new, independent Civil Liberties and Privacy Tribunal was promised to exercise some substantial oversight – however, this was not enshrined in the eventual Act, and has by now been abandoned.

The Lib Dem leadership and their government ministers endorsed the Bill, the constitutionality of the process by which it was enacted, and its interpretation by the Home Office in the face of considerable opposition by their own followers. This position became even more difficult to maintain when two MPs, from Labour and the Tory party, mounted a successful legal challenge to the High Court. On the 17th July 2015, in *David Davis and others v Secretary of State for the Home Department*, the court ruled that DRIP was incompatible with EU privacy and human rights law.[15] The decision, which is

[11] IPT judgement IPT/13/77/H http://www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

[12] IPT/13/77/H. For a critical analysis of both rulings see Bernal, P, (2015). Liberty and others vs. GCHQ and others, Jusletter-IT http://jusletter-it.weblaw.ch/en/issues/2015/24-September-2015.html.

[13] https://www.liberty-human-rights.org.uk/news/blog/drip-effect

[14] See e.g. Grossman, W.M. " Emergency" Ushers in a New Era in British Communications Surveillance. *IEEE Security & Privacy* 6 (2014): 84-88;

[15] https://www.judiciary.gov.uk/wp-content/uploads/2015/07/davis_judgment.pdf

under appeal by the government, ordered that sections 1 and 2 be not applied, but suspended the enforcement of the decision until 31 March 2016. The purpose is to give the government the option to redraft the section to make it compatible with EU law.

It was against this background that the country went into a general election. The Lib Dems had prevented the "Snooper's Charta" in 2012, but the more recent memory for their voters and grassroots members was their acquiescence to DRIP and their support for a process that played at the very least fast and loose with the constitution, and compromised the role of Parliament. The Snowden revelations, which at any other time could have boosted their support as a rallying point for civil liberty and privacy advocates, wrong-footed them entirely. As junior partner in a conservative government, they had little leeway in mounting an overt confrontation with the Home Office or to criticize the government without formally leaving the coalition. The punishment by the electorate was brutal and eliminated them as a power in UK politics. They lost 49 of their 57 seats, and while civil liberty and DRIP was only one amongst several reasons, it contributed considerably to the dissatisfaction amongst their own supporters. One result of the collapse of the Lib Dem vote was an absolute majority for the conservatives, who now faced the task of addressing the law on data retention unencumbered by a coalition partner.

As of summer of 2015, the UK legal framework on data collection and police surveillance was in tatters. The sunset clause of DRIPA meant action was needed to keep the data retention capabilities of the UK security services, even without the High Court challenge. The report by the Reviewer of Terrorism Legislation had painted a dire picture of the efficiency of RIPA and the bodies charged with enforcing/supervising it, declaring the need for a root and branch revision of a failing system never fit for its purpose: neither sufficiently clearly allowing forms of surveillance deemed necessary by the security services, nor providing a robust supervisory mechanism that would ensure that the police and security services used their legal powers correctly. Snowden had shown that the UK security services either ignored the legal framework altogether, or used an overly wide interpretation of the law. The CJEU had called into question the legality of all forms of undirected bulk surveillance.

In this political environment, the Home Office revived the 2013 Draft Communications Data Bill, combining the data retention and mass surveillance powers proposed then with a new and, arguably, more stringent form of judicial control and a more streamlined oversight regime. Rather than following the lead of the CJEU and indeed the UK Investigatory Powers Tribunal, the answer was to further extend surveillance powers, *but* this time with a proper legal basis and formal process of judicial supervision. As with DRIP, the government continued the policy of minimizing substantial parliamentary oversight wherever possible. A first draft for consultation was published late in November 2015, with a proposed first reading of the Bill in February 2016. This gave MPs, parliamentary committees and NGOs just little over two months – and over the Christmas holidays – to digest and analyze a mammoth Bill of over 200 pages, and with over 400 pages of further codes of practice.

Despite this short time frame, public criticism both from within and outside parliament quickly mounted. The Joint Select Committee for the Investigatory Powers Bill, the parliamentary committee charged with conducting the public consultation, received 148 submissions, running to over 1500 pages, most of them highly critical of both the procedure of enactment and the substance of the proposal.[16] The committee itself recommended in its report 86 partly substantial changes.[17] The Intelligence and Security Committee, chaired by a former Attorney General and generally friendly towards the security services was even more scathing. It noted that the committee had endorsed the principle of bulk data retention in its earlier report, *Privacy and Security: A modern and transparent legal framework,* provided a suitable regulatory environment was created. [18] On the proposal, it notes:[19]

"The Committee is disappointed to note that it does not cover all the Agencies' intrusive capabilities. [...]. This is – in our view – a significant missed opportunity"

Regarding privacy in particular, it states that "Overall, the privacy protections are inconsistent and in our view need strengthening." The government's reaction to these criticisms of the privacy regime of the Bill was one of contempt – it added the word "privacy" to the header of the Bill that introduces the judicial warrant requirement.

.

3 The IPB: The main features

As we saw, the IPB pursues a threefold aim. First, it consolidates existing police powers, regulated currently by a number of specific laws, in one piece of legislation. Second, it "updates" these powers to bring them in line with the "digital age" – in the words of the government, to "restore capabilities that have been lost as a result of changes in the way people communicate". [20] Third, it also consolidates several supervisory bodies, including the Interception of Communications Commissioner and the Chief Surveillance Commissioner (CSC) in one new agency, the Investigatory Powers Commissioner (IPC) whose role it will be to oversee how these powers are used.

These three main aims – consolidation, authorisation, and regulation, can help us to structure the more detailed provisions that the Bill proposes.

Consolidation: The IPB combines police powers currently exercised either under the Regulation of Investigatory Powers Act (RIPA), the Wireless Telegraphy Act 2006 or the Data Retention and Investigatory Powers Act (DRIPA) 2014 as the main authorizing provisions. Other piecemeal powers that are affected are sec 94 of the Telecommunications Act 1984 (particular important for our discussion below, as it empowered the Secretary of State to give "directions" to telecommunication providers, which could include requests for technological

[16] http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf

[17] http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/9302.htm

[18] isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf

[19] http://isc.independent.gov.uk/files/20160209_ISC_Rpt_IPBill(web).pdf p 5-6

[20] Foreword to the Investigatory Powers Bill by the Home Secretary, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf at p. 5.

assistance); the Justice and Security Act 2013; sections 15 and 16 of the Police and Criminal Evidence Act 1984 (PACE); and section 37 of the Supreme Courts Act 1981. The last two are general powers of UK courts to grant search orders, which can include searching and seizing computer equipment and files. Affected are also powers given under the Intelligence Services Act (ISA) 1994 – these pertain to the authorisation of "computer network exploitation" or hacking..

Authorisation: This aspect of the Bill is unsurprisingly the most contentious, creating far reaching new powers for the police and duties for communication service providers. In particular, the Bill lays out the conditions and procedures under which warrants can be obtained for

- the interception of communications,
- the mandatory retention and acquisition of communications data,
- equipment interference (hacking)
- the retention and examination of bulk personal datasets.
- "filter search" across several data sets

In each of these cases, warrants can be obtained for targeted and bulk surveillance, including bulk hacking which could compromise entire communication networks. CSPs can be compelled to assist in the hacking of accounts of their customers, and it seems possible that third parties with relevant expertise can be drafted into assisting the police and security services. This aspect of the Bill echoes the use of the ancient "All Writs Act" in the recent litigation between Apple and the FBI, or even more the subsequent legislative proposal by senators Burr and Feinstein, the "Compliance with Court Orders Act of 2016," which would enable courts to force any third party to assist police in circumventing encryption or similar privacy and security enhancing methods.[21] The IPB also creates a new criminal offence of disclosing data requests made under the IPB to the target of the investigation, third parties or the public – potentially criminalizing whistleblowing. In this respect the IPBs approach to privacy falls well behind even the normal US attitude whose reliance on the political process permits greater transparency.

The data retention warrant will require communication service providers to retain "Internet connection records" – the meta-data of which websites were visited for all UK users, and for 12 months duration. The particular pages and the full browsing history will not be kept. While warrants for various surveillance activities are at the heart of the Bill, police and intelligence officers will have the right to see these records as part of a targeted and filtered investigation, without a warrant.

Warrants can be obtained if this is

1. in the interest of national security;
2. needed for preventing or detecting serious crime;
3. required to fulfil duties under a mutual assistance agreement with a foreign agency;
4. safeguarding the economic well-being of the UK (in circumstances relevant to the interests of national security)

1) and 2) are ill defined and have in the past been interpreted broadly by police (regarding "seriousness" of crime) and security services (regarding the term "national interest". 3) could, as in the past, circumvent domestic legal restraints – sharing data with the US that does not meet any of the other requirements, only to receive it "back" again from them. 4) is the revised version of a corresponding clause in RIPA, which had resulted in particularly problematic abuse of surveillance powers. The Bill improves the existing situation to a degree here, by clarifying that the economic interests must be important enough to be of relevance for national security – though what this then adds to 1) remains unclear.

Control: While the IPB widens considerable the surveillance powers of police and security services, the "deal" that was suggested by the Reviewer of Terrorism legislation was to balance this by a more stringent system of approvals and supervision. The Bill follows this suggestion to a degree. It simplifies and strengthens the supervisory regime, as indicated, by uniting the roles of several agencies in the hand of one new body, the Investigatory Powers Commission which will combine and replace the powers of the current Interception of Communications Commissioner, Intelligence Services Commissioner, and Chief Surveillance Commissioner. The Intelligence and Security Committee of Parliament and the Investigatory Powers Tribunal retain their various roles.

The IPC will consist of a number of serving or former senior judges, the Judicial Commissioners. Its main role will be to provide a so called "double lock": while under RIPA a politician, the Home Secretary, signs off on all warrants, under the IPB, both the signature of a Judicial Commissioner and the Home Secretary are needed. In addition to the authorization of investigatory activities, the IPC will also have an inspection role and far reaching freedom to define the scope and process of this inspection process. The IPC will audit compliance and undertake investigations. However, the Bill is silent on the powers the IPC will have to compel the cooperation of security services or police. Finally, the Commissioner will have a mandate to inform Parliament and the public about the need for and use of investigatory powers. The Bill mandates that the Prime Minister appoints the Information Powers Commissioner – but gives him/her discretion as to the number of other commissioners that will be appointed, leaving the agency potentially overworked.

Given the central role of the IPC Commissioner, the appointment process also raises the same constitutional issue that we discussed above regarding DRIP: while the Prime Minister has to consult with and inform the heads of the Scottish, Irish and Welsh devolved executives, they have no veto over the appointment or any other direct influence in the appointment process. The UK parliament too remains sidelined – it neither plays a role in the appointment process nor can it call the IPC to account.

4 Evaluation and outlook: a view from the outside

The IPB undoubtedly increases the surveillance capabilities of British police and security services considerably – or expressed more cautiously, puts capabilities that have been used for some time now on a legal footing. Privacy advocates can find some consolation in a strengthened and more transparent supervisory system, where politicians at least have to share some of the power with independent judges. But the IPB does not only affect the UK. Just as with DRIP, some of its provisions create an extraterritorial reach of UK surveillance law, in

[21] https://josephhall.org/f0eabaa89b8ee38577bf7d0fd50ddf0d58ecd27a/307378123-Burr-Encryption-Bill-Discussion-Draft.pdf

particular vis-à-vis UK domiciled companies with international business. For the UN, the special rapporteur on privacy heavily criticised the Bill, expressing his hope "that disproportionate, privacy-intrusive measures such as bulk surveillance and bulk hacking as contemplated in the investigatory powers bill be outlawed rather an legitimised."[22] This for sure was the lesson other EU countries took from *Digital Rights Ireland*.

The question though is, does this still matter? On June 23.6.2016, the UK decided with a 51.9% to 48.1 majority to end its membership of the EU. Since then, the Prime Minister has resigned, and while the necessary Art 50 notification that triggers the two year negotiation process has not yet been issued, it seems inevitable now that the UK will leave the Union sooner or later. Crucially, though, it is at this point unknown what the negotiation position of the UK will be, or indeed if it will emerge only after a general election is called.

Several outcomes are possible. In one scenario, the UK remains member of the EEA in a position similar to Norway. In this case, the UK would have to observe all relevant EU regulations. It is at least questionable if the IPB is compliant with EU Data Protection law, even though civil servants have pointed out privately to the author that this was an explicit goal, and one reason for adding substantial new procedural safeguards. This emphasis of "post collection" safeguards in data use however, much in line with the US reliance on 4th Amendment restraints, misreads partly the European concern with bulk data collection. The UK also struggles to see privacy mainly as an Art 8 human right, and focus almost exclusively on more technical compliance issues with the Data Protection Directive. the British exit means that the country will not any longer be subject to the jurisdiction of the European Court of Justice, but leaving aside the possibility that the UK could also withdraw from the ECHR – an idea that was in the past mooted by the Home Secretary, now frontrunner to become the next Prime Minister – the UK would still need to observe the evolving EU understanding of privacy as a human right, either through the ECHR case law or in order to maintain access to the EEA. In fact, the UK withdrawal could also mean in a stronger and faster development of EU Data Protection law, the UK having been in the past one of the more industry and police friendly negotiators.

The most radical scenario, favoured by the UK Independence Party, is a "full brexit", with the relation between the UK and Europe governed solely by WTO rules. In this case, the EU and UK would have to negotiate a separate "Privacy Shield" agreement if data sharing remains possible – something the UK cannot possibly afford to forgo. In *Schrems v Data Protection Commissioner,*[23] the CJEU had ruled the safe harbour agreement with the US invalid. Mass retention of data and the data sharing arrangements with the police were at the core of the decision.[24] The IPB provides for the same powers. And even though it introduces judicial oversight, these too remain if anything weaker than their US counterparts. Privacy Shield, the successor agreement to Safe Harbour, was published the same month as the IPB reached parliament. Despite concerns by privacy advocates, even a weak Privacy Shield seems incompatible with the IPB. Bulk data collection is discouraged, and where permitted then only to counter six explicitly defined serious threats, a much narrower range than provided under the IPB and its "economic interest" test.[25]

Even if we assume that Privacy Shield passes scrutiny by the CJEU, the UK and the IPB would struggle to be seen PS-compliant. At the same time, a UK-EU agreement could be more demanding than PS. Unlike the US, the `UK has no economic leverage – EU citizens do not depend on UK platforms the way they depend on Facebook or Twitter, and the US does not depend on the UK market the same way it needs access to the EU.[26] The UK would likely struggle to negotiate a deal as generous as Privacy Shield. This leaves the administration heavy and costly solution of using the EU Model clauses for Data Transfer. In the meantime UK companies are likely to pre-empt the negotiations by setting up independent subsidiaries on the continent – following the example of US companies after *Schrems*. Many data-intensive industries, in particular the banking sector, are likely to favour this move anyway once free movement of services stops. The IPB permits bulk data collection "if needed to prevent economic harm" to the UK – it would be a supreme irony if the IPB turned out to be a major threat to what is currently the largest Internet economy of the G20.[27]

[22] http://www.wired.co.uk/news/archive/2015-11/10/surveillance-investigatory-powers-scary-joseph-cannataci

[23] Judgment in Case C-362/14.

[24] Loideain, N N. (2015). EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era. *Media and Communication*, *3*(2).

[25] COMMISSION IMPLEMENTING DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield sec. 69

[26] For a more comprehensive and very insightful analysis, see Taylor, E (2016) 'Brexit' Could Put Data Sharing in Jeopardy, https://www.chathamhouse.org/expert/comment/brexit-could-put-data-sharing-jeopardy.

[27] http://www.consultancy.uk/news/1988/bcg-uk-internet-economy-the-largest-of-the-g20