Human Rights Law Clinic Papers 2017

THE HUMAN RIGHTS IMPLICATIONS OF MASS SURVEILLANCE AND DATA COLLECTION

To: Lisa Oldring, UN Office of the High Commissioner for Human Rights

Submitted by: Bradley Kershaw

May 2017

UNIVERSITY OF SUSSEX

Sussex Law School Human Rights Law Clinic

The Human Rights Law Clinic operates as an optional module in the LLM degree in International Human Rights Law at Sussex Law School at the University of Sussex. The Clinic offers students the chance to build on law and theory through the preparation of pro bono legal opinions for clients. Students work under the supervision of the Clinic's convenor, an academic and practitioner in human rights, on specific legal questions related to international human rights law coming from clients. Depending on the complexity and nature of the legal opinions sought, students work individually or in small groups to produce memoranda for their clients, following a process of consultation with clients, close supervision, oversight and review by the Clinic's convenor, seminar discussions on work in progress, and presentations to clients of draft memoranda.

www.sussex.ac.uk/schrr/clinic

Sussex Centre for Human Rights Research

Sussex Law School's Sussex Centre for Human Rights Research aims to foster a vibrant research culture for human rights researchers within the Sussex Law School. Its work has a global as well as national focus and its researchers adopt a range of approaches to human rights research (e.g. doctrinal, critical, theoretical, practical and inter-disciplinary). The Human Rights Law Clinic operates in pursuit of the Centre's objectives to feed into human rights debates and collaborate with relevant organisations, locally, nationally and internationally; and to attract and give opportunities to high-quality postgraduate students.

www.sussex.ac.uk/schrr

Contents

Introduction

Digital communications and online interaction have become enriching staples of contemporary life.[1] However, since the revelations of Edward Snowden in 2013 rights-proponents have been deeply concerned by the opportunities contemporary communication afford to States to gather inordinate amounts of personal data, potentially endangering a plethora of fundamental human-rights.[2] Mass surveillance has become a 'dangerous habit' of governments,[3] enabled by the private sector[4] and a lack of effective and transparent oversight of these activities.[5] Today, the Internet carries communications of 2.4 billion users transferring 1.5 million gigabytes of data which is vulnerable to a multitude of tools employed by States, including front-door access to service providers, fibre-optic cable tapping, interception and hacking potentially leading to collection, retention and analysis of a disproportionate quantity of personal data.[6]

Mass surveillance is a sweeping phrase, with States preferring to employ the phrase 'bulk' powers,[7] but the issue is very much one of semantics with each acting as shorthand for the 'gathering of massive amounts of data'.[8] These activities risk a disproportionate and unnecessary number of individuals becoming the subject of mass surveillance and having their rights illegitimately interfered with.[9] What is required to combat this are transparent and effective oversight regimes operating in administrative, judicial and parliamentary spectrums[10] to safeguard against arbitrariness[11] and to create benchmarks ensuring legality,[12] necessity and proportionality.[13] Therefore, this memorandum scrutinises the efficacy of domestic oversight bodies and the implications of the increasing role of the private sector in data-gathering.

Rights affected and regional policy approaches

The right most palpably affected by mass surveillance is clearly the right to privacy. Article 17 of the International Covenant on Civil and Political Rights (ICCPR)[14] prohibits arbitrary or unlawful interference with the right to privacy and requires any intrusion upon privacy to be pursuant to the law.[15] Therefore, any surveillance regime must be in accordance with law and proportionate to a legitimate end that is necessary in the circumstances.[16] These

[1] OHCHR, 'The right to privacy in the digital age', UN Doc A/HRC/27/37 (2014), paras 1-2.
[2] Pieter Omtzigt, 'Mass Surveillance' Council of Europe Committee on Legal Affairs and Human Rights Report AS/Jur (2015) 01 1, 4; OHCHR report 2014, ibid, para 2; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/23/40 (2013), para 33; Paul Bernal, 'Data gathering, surveillance and human rights: recasting the debate' (2016) 1(2) *Journal of Cyber Policy* 243, 246-247.
[3] OHCHR report, op cit, para 3.
[4] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/32/38 (2016), para 1.
[5] Omtzigt, op cit, 7.
[6] Intelligence and Security Committee of Parliament, 'Privacy and Security: A modern and transparent legal framework', HC 1075, 12 March 2015, 26; Omtzigt, op cit, 6-7.
[7] For example, see the Investigatory Powers Act 2016, Parts 5, 6 and 7.
[8] Bernal, op cit, 246-247.
[9] Ibid.
[10] Omtzigt, op cit, 25.
[11] *Roman Zakharov v Russia*, ECtHR App No. 47143/06, judgment of 4 December 2015, para 270.
[12] Report of the Special Rapporteur on the right to privacy, UN Doc A/HRC/31/64 (2016), para 38.
[13] Joint Committee on Human Rights, 'Legislative Scrutiny: Investigatory Powers Bill' First Report of Session 2016 – 2017, HL Paper 6 HC 104, 2 June 2016, 6.
[14] See also the Universal Declaration of Human Rights, adopted under UNGA Res 217 A(III)) (1948), Article 12.
[15] ICCPR, Article 17(1)-(2); UDHR, Article 12; Report of the Special Rapporteur on the right to privacy (2016), op cit, 20; OHCHR, Status of Ratification: Interactive Dashboard, available at URL <http://indicators.ohchr/org/> (accessed 21 March 2017), 169 States parties are signed up to the ICCPR.
[16] UN Human Rights Committee, General Comment No.16: Article 17 (Right to Privacy) (1988), available at URL <http://tbinternet.ohchr.org/_layouts/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=11> (accessed 26 April 2017) paras 3-4.

protections are also enshrined in regional rights treaties,[17] such as the European Convention on Human Rights (ECHR)[18] and European Charter of Fundamental Rights and Freedoms (CFREU).[19] However, it must be acknowledged that mass surveillance impacts a 'wide range of human-rights' outside of privacy.[20]

Other affected rights

Individuals increasingly express themselves through digital media,[21] and evidence gathered illustrates a chilling effect on free expression[22] due to mass surveillance methods.[23] In the field of journalism a PEN survey highlighted a contemporary trend of 'self-censorship' with 24 per cent of respondents stating they avoid writing about certain topics in the wake of Snowden.[24] The corollary right of freedom to receive information is also impacted upon,[25] with indiscriminate collection potentially compromising security of journalistic sources and deterring those sources from coming forward.[26] Privacy and free expression in that regard are mutually dependant as one may refrain from saying something they would with guarantees of anonymity.[27]

Freedom of association[28] is also impacted upon with evidence suggesting governments around the world utilise mass surveillance techniques to monitor the activities of potential dissidents, protestors[29] and revolutionary actors.[30] Not only does this lead to a stifling of association and assembly in the moment, but the mere knowledge of these abilities may lead to more conformist behaviour in general from such groups; impeding their work and membership.[31]

Mass surveillance can also impact on the right to a fair trial.[32] Indiscriminate collection could lead to the collection of data containing privileged communications between an individual and their legal counsel,[33] potentially having a 'chilling effect' on vital free and frank lawyer-client communications.[34] Mass surveillance may even circumvent, to an extent, due process guarantees. In *Kadi*, for example, the Court of Justice of the European Union (ECJ)

[17] OHCHR report, op cit, para 13.
[18] Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (European Convention on Human Rights, as amended), Article 8.
[19] Charter of Fundamental Rights of the European Union, Article 7 (right to privacy), Article 8 (personal data protection).
[20] Bernal, op cit, 245; OHCHR report, op cit, 14.
[21] OHCHR report, ibid; Report of the Special Rapporteur on the freedom of expression, op cit, para 6.
[22] Protected under ICCPR Article 19.
[23] Report of the Special Rapporteur on the freedom of expression, op cit, para 6; Omtzigt, op cit, 1; OHCHR report, op cit, para 14; *Weber and Saravia v Germany*, ECtHR App No. 54934/00, judgment of 29 June 2006, para 349.
[24] Omtzigt, op cit, 25; Pen-International, 'Chilling Effects: NSA Surveillance Drives Writers to Self-Censor' (pen-international, 2013), at URL <http://www.pen-international.org/read-pen-american-centres-report-chilling-effects-nsa-surveillance-drives-writers-to-self-censor/> (accessed 22 March 2017).
[25] ICCPR Article 19(2); ECHR Article 10.
[26] Bernal, op cit, 254.
[27] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/23/40 (2013), para 79.
[28] ICCPR Article 22; ECHR Article 11.
[29] Brian Wheeler, 'Whitehall chiefs scan Twitter to head off badger protests' (BBC London, 20 June 2013), at URL <http://www.bbc.co.uk/news/uk-politics-22984367> (accessed 22 March 2017).
[30] Bernal, op cit, 256.
[31] Bernal, op cit, 256-57; Electronic Frontier Foundation, 'EFF Files 22 Firsthand Accounts of How NSA Surveillance Chilled the Right to Association' (Electronic Frontier Foundation, 6 November 2013), at URL <https://www.eff.org/press/releases/eff-files-22-firsthand-accounts-how-nsa-surveillance-chilled-right-association> (accessed 22 March 2017).
[32] ICCPR Article 14.
[33] Bernal, op cit, 255-256.
[34] Bernal, op cit, 256; The Bar Council, 'The Bar Council in Parliament this week…' (1 July 2016), at URL <http://www.barcouncil.org.uk/media-centre/news-and-press-releases/2016/july/the-bar-council-in-parliament-this-week-/> (accessed 22 March 2017).

highlighted concerns of rights-proponents about the impact of mass surveillance on the presumption of innocence and the undermining of a fair trial.[35]

These rights, however, are not absolute with the exception of certain elements of right to a fair trial. International human rights law (IHRL) allows for explicit legitimate aims to interfere with qualified rights.[36] However, such infringements must always be legal, necessary and proportionate.[37] What is legal, necessary and proportionate in mass surveillance practices has been elucidated through 'regional-policy approaches', most acutely by the European Court of Human Rights (ECtHR) and ECJ.[38] These standards should be at the forefront of considerations for domestic oversight mechanisms.

Policy approaches

Mass surveillance has three stages: data gathering; automated analysis; and human analysis.[39] States purport to exclude their mass gathering techniques from scrutiny by stating questions of rights occur only at the final human intervention stage, and that what was collected is merely metadata and is thus not rights-infringing.[40]

Regional developments, however, have put paid to these notions in finding that the mere occurrence of surveillance is a harm in itself; that 'mere retention and storing of personal data' were regarded as directly impacting on human rights and liberty,[41] and that metadata taken as a whole allows for 'very precise conclusions' to be drawn about an individual's life, unquestionably engaging their human rights.[42] European bodies have contemporarily been reining in surveillance practices of States to a point where it may now be said that indiscriminate gathering of data is prohibited[43] repudiating notions serious crime and national security threats give States a blank cheque for surveillance, pressing for clarity,[44] necessity and oversight within State laws.[45]

Recently, however, two decisions in the ECJ (*Digital Rights Ireland* and *Watson*),[46] and two decisions in the ECtHR (*Zakharov* and *Szabó*) may well have set the gold standard for State surveillance.[47] In *Digital*, the ECJ invalidated the Data Retention Directive[48] as infringing

[35] *Kadi and Al Barakaat* [2008] ECR. I-6351; Bernal, op cit, 256; Federico Fabbrini, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its lessons for Privacy and Surveillance in the US' (2015) 28 *Harvard Human Rights Journal* 65, 84.
[36] For example, ECHR Article 8(2); European Charter Articles 8(2) and 52.
[37] OHCHR report, op cit, para 23; reinforced in the field of surveillance by UNGA Res 68/167 (2014).
[38] Report of the Special Rapporteur on privacy (2016), op cit, para 35; OHCHR report, op cit, para 38.
[39] Bernal, op cit, 249.
[40] Ibid.
[41] *S and Marper v United Kingdom* [2008] ECHR 1581, para 121; *Klass and others v Germany* [1978] ECHR 4, para 41; Quentin Skinner and Richard Marshall, 'Liberty, Liberalism and Surveillance: a historic overview' (openDemocracy U, 26 July 2013), at URL <https://www.opendemocracy.net/ourkingdom/quentin-skinner-richard-marshall/liberty-liberalism-and-surveillance-historic-overview> (accessed 25 March 2017).
[42] *Digital Rights Ireland Ltd v Minister for Communication* [2014] ECR I-238, paras 26-27 and 37; *Weber*, op cit, para 78; *Malone v United Kingdom*, ECtHR App No. 8691/79, judgment of 2 August 1984, para 64.
[43] Sarah St. Vincent, 'Did the European Court of Human Rights Just Outlaw "Massive Monitoring of Communications" in Europe?' (Centre for Democracy and Technology, 13 January 2016), at URL <https://cdt.org/blog/did-the-european-court-of-human-rights-just-outlaw-massive-monitoring-of-communications-in-europe/> (accessed 10 March 2017); Martha Spurrier, 'Surveillance has gone too far. The jig is up' (The Guardian London, 22 December 2016), at URL <https://www.theguardian.com/commentisfree/2016/dec/22/government-surveillance-eu-court-ruling-investigatory-powers-act-private-lives> (accessed 4 March 2017).
[44] Fabbrini, op cit, 84.
[45] *Klass*, op cit; *Weber*, op cit; *Liberty v United Kingdom*, ECtHR App No. 58243/00, judgment of 1 July 2008; *Kennedy v United Kingdom*, ECtHR App No. 26839/05, judgment of 18 May 2010; *Google Spain v Agencia Espanola de Proteccion de Datos*, Case C-131/12, ECtHR Grand Chamber, judgment of 13 May 2014; Omtzigt, op cit, 11.
[46] *Digital Rights Ireland*, op cit; *Tele2 Sverige AB v Post-Och Telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and others,* ECtHR Joined Cases C-203/15 and C-698/15, judgment of 21 December 2016; Report of the Special Rapporteur on the right to privacy, UN Doc A/HRC/34/60 (2017), para 14.
[47] *Szabó and Vissy v Hungary*, ECtHR App No. 37138/14, judgment of 12 January 2016; *Zakharov*, op cit.

protections on privacy[49] and personal data[50] owing to its allowances for indiscriminate collection or retention of data,[51] lack of sufficient legitimate aims sanctioning surveillance and data collection[52] and lack of a restrictive timeframe for retention of that data.[53] Critically, it held that a lack of accompanying safeguards and oversight tends toward a disproportionate regime.[54] This was buttressed in *Watson*, where the ECJ again criticised indiscriminate mass surveillance regimes.[55] Concurrently, the ECtHR in *Zakharov* began a process of requiring individualisation of surveillance regimes,[56] then declaring in *Szabó* that surveillance could only be proportionate when utilised in an individual operation,[57] an approach set for further clarification in pending applications before the ECtHR.[58]

However, this approach can only be revolutionary if States follow it or cannot tease out a soft reading. In the wake of *Digital*, for example, certain Member State's national courts annulled[59] or suspended national data retention laws.[60] In juxtaposition, some governments have read *Digital* as not banning mass surveillance per se, but rather that mass surveillance must be accompanied by appropriate safeguards; a permissive reading.[61] This approach was epitomised in the UK with the Government emphasising that if a State had robust oversight in place then a mass surveillance regime could settle with the finding in *Digital* and likely later decisions.[62]

Oversight and accountability: the United Kingdom, United States and the private sphere

The UK approach might be treated as an admission that oversight 'underpins' the lawfulness of surveillance regimes.[63] Furthermore, even a soft reading of current regional decisions, such as *Zakharov*, place an increasing emphasis on the legality of State surveillance practice being tied to effectiveness of oversight.[64] Contemporary mass surveillance maladies may have been the result of a lack of efficient oversight within States leading the Special Rapporteur on privacy to proclaim in 2017 'the most promising avenue for concrete measures to protect [rights]' in the field of surveillance and data-gathering will be effective oversight.[65] The Special Rapporteur's focus on evolved discussions on how to structure oversight leads to a prima facie inference current standards are ineffective.[66]

Effective oversight entails the presence of mechanisms that are independent, adequately resourced, impartial and transparent, operating across administrative, judicial and

[48] Data Retention Directive, Directive 2006/24/EC (15 March 2006).
[49] European Charter Article 7.
[50] Ibid Article 8.
[51] *Digital Rights Ireland*, op cit, para 58.
[52] Ibid, para 60.
[53] Ibid, para 63.
[54] Ibid, paras 66 and 69.
[55] *Watson*, op cit, para103.
[56] St. Vincent, op cit.
[57] Ibid.
[58] *Brever v Germany*, ECtHR App No. 50001/12 (application communicated 21 March 2016); *Calovic v Montenegro*, ECtHR App No. 18667/11 (application communicated 31 March 2016).
[59] Niklas Vainio and Samuli Miettinen, 'Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the member states' (2015) 23 *International Journal of Law and Information Technology* 290, 301-303. For example, see the Austrian Constitutional Court, Romanian Constitutional Court and Constitutional Court of the Republic of Slovenia, Bulgarian Supreme Administrative Court, and the District Court of the Hague in the Netherlands.
[60] Vainio, op cit, 301-303, for example the Slovakian Constitutional Court.
[61] Ibid, 303.
[62] Ibid, 304.
[63] Report of the Special Rapporteur on privacy (2016), op cit, para 7.
[64] *Zakharov*, op cit, para 233; Joint Committee on Human Rights, op cit, 12.
[65] Report of the Special Rapporteur on privacy (2017), op cit, para 3.
[66] OHCHR report, op cit, para 37.

parliamentary spectrums,[67] providing ex ante authorisation and ex post verification and review.[68] In that way, the human rights implications of mass surveillance can only be as great as these bodies permit. This memorandum will focus on the systems of oversight in the UK and USA owing to the regard some commentators have for their efficiency[69] and owing to the fact that they were among the worst alleged perpetrators of mass surveillance in the Snowden leaks. The question investigated will be *why* mass surveillance was able to runaway in these States in spite of sophisticated oversight, and what form oversight structures should take in the future to counter this and earn public trust.[70]

The United Kingdom

The UK's oversight system is undergoing extensive changes with the passing into law of the Investigatory Powers Act 2016 (IPA).[71] However, the system had its foundations laid under the Regulation of Investigatory Powers Act 2000 (RIPA) and the Data-Retention and Investigatory Powers Act 2014 (DRIPA).The oversight structures in the UK up to this point were complex,[72] consisting of three Commissioners,[73] a parliamentary oversight regime mainly in the form of the Intelligence and Security Committee (ISC) and a judicial complaints handler in the Investigatory Powers Tribunal (IPT).[74]

Pre-IPA mechanisms

The UK refers to its own mass surveillance and data gathering regimes as bulk practices, piling up data 'haystacks' to find 'needles' of interests.[75] This process was, and will continue to be, governed by a system of warrants[76] and the condition that only external communications (with one end abroad) can be collected in these bulk regimes, while wholly domestic communications (both ends in the UK) cannot.[77]

Therefore, oversight was predicated on warrant approval. However, authorisation came from the Home Secretary[78] who declared that human rights concerns, such as necessity and proportionality, were part of the consideration process while also admitting that bulk warrants were treated differently from targeted surveillance warrants.[79] Targeted warrants had very specific safeguards and tests,[80] whereas bulk warrants were issued with *some* built-in human rights checks, albeit that the Joint Committee on Human Rights assessed that it is 'probably impossible' to carry out an effective proportionality test on bulk powers.[81] Further, ministerial approval seems contrary to principles of independence, impartiality and

[67] UNGA Res 68/167 (2014), para 4(d).
[68] Report of the Special Rapporteur on privacy (2017), op cit, para 25; Ian Brown, 'The Feasibility of transatlantic privacy-protective standards for surveillance' (2015) 23(1) *International Journal of Law and Information Technology* 23, 32.
[69] Ashley Deeks, 'An International Legal Framework for Surveillance' (2015) 55(2) *Virginia Journal of International Law* 291, 345.
[70] David Anderson QC, 'A Question of Trust: Report of the Investigatory Powers Review' (June 2015), at URL <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf> (accessed 21 March 2017), para 13.3.
[71] Joint Committee on Human Rights, op cit, 29.
[72] Commissioner for Human Rights for the Council of Europe, 'Memorandum on Surveillance and Oversight Mechanisms in the United Kingdom', CommDH(2016)20 (Strasbourg, 17 May 2016), at URL <http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806db72c> (accessed 10 February 2017), para 5.
[73] Interception of Communications Commissioner, Surveillance Commissioner, and the Intelligence Services Commissioner.
[74] Commissioner for Council of Europe, op cit, para 7.
[75] Intelligence and Security Committee, op cit, 25.
[76] Previously, Regulation of Investigatory Powers Act 2000, section 8(4); replaced by Investigatory Powers Act 2016, Parts 6 and 7.
[77] Intelligence and Security Committee, op cit, 39.
[78] Regulation of Investigatory Powers Act 2000, section 8(4).
[79] Ibid, section 8(1); Intelligence and Security Committee, op cit, 37.
[80] Intelligence and Security Committee, op cit, 17-23.
[81] Joint Committee on Human Rights, op cit. 10-11.

transparency. Accompanying the warrants are certificates regulating the usage of data gathered, but these are couched in vague terms meaning operational discretion was given to agencies and therefore primacy was placed in their internal safeguards.[82]

Evidence of the dangerous effect this opaque system, described as 'biased' by the ISC,[83] is found in evidence to an ISC report where confused exposition from ministers and intelligence figures obfuscated the external-internal distinction by seeming to state that 'all' Internet communications were regarded as external, meaning that function-creep had occurred, potentially leading to an inordinate amount of data being collected in these bulk dragnets.[84] This leads to an inference that those internal safeguards had, at best, been remiss in evolving with digital realities. Worse still, collection of bulk-personal-datasets (large databases containing personal information about a range of people) had no statutory footing at all, meaning there were no explicit restrictions or authorisation procedures outside of internal agency regulation.[85]

For oversight independent of the ministerial or agency setting, one looks to the Commissioners. However, these Commissioners carried out only retrospective audit, on a part-time basis,[86] in total secrecy, lacking resourcing and employing a 'sampling' regime on an insufficient body of ministerial and agency work.[87] The Commissioners were also appointed by the Prime Minister; an unnecessary potential compromising of their independence.

Parliamentary scrutiny of intelligence activities was mainly provided by the ISC.[88] One relies on their reports for clarification on these oversight powers, which the ISC itself concluded were dated, inefficient and unnecessarily complex.[89] However, again, this vital body was under-resourced with a permanent staff of six. Worse still, its membership was subject to veto by the Prime Minister, as was the work it undertook.[90]

The final limb of this convoluted oversight system is the IPT,[91] a panel of judges and lawyers mandated to hear complaints of wrongful interference from surveillance authorised through the procedures outlined.[92] Part of its mandate was to take into consideration allegations of human rights infringements and rights-implications of decisions taken by authorities.[93] In its provision of remedies, however, the IPT was reliant on ex post notification to surveillance subjects,[94] whereas such notification is treated with caution by States[95] as potentially leading to revelation of agency methods and the undermining of investigations.[96] However, when fully informed applicants have made petitions to the IPT, the Tribunal was able to deliver

[82] Intelligence and Security Committee, op cit, 27-30 and 37.
[83] Ibid, 74.
[84] Ibid, 39-40.
[85] Ibid, 57-58.
[86] Ibid, 77.
[87] Intelligence and Security Committee, op cit, 78.
[88] Commissioner for Council of Europe, op cit, para7; only having its remit expanded to cover oversight and operational activities through Justice and Security Act 2013.
[89] Intelligence and Security Committee, op cit; similar conclusions were also drawn by Anderson QC, op cit; and, Royal United Services Institute, 'A Democratic Licence to Operate: Report of the Independent Surveillance Review' (July 2015), at URL <https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf> (accessed 26 March /2017).
[90] Commissioner for Council of Europe, op cit, paras 9-10.
[91] Investigatory Powers Tribunal, established pursuant to Regulation of Investigatory Powers Act 2000, section 65(1).
[92] Commissioner for Council of Europe, op cit, para 11.
[93] Ibid, para 11; Intelligence and Security Committee, op cit, 78.
[94] Peter Margulies, 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism' (2014) 82(5) *Fordham Law Review* 2137, 2162.
[95] Ibid, 2162.
[96] *Weber*, op cit, para 345.

decisions of infringements of rights-standards in agency practice,[97] leading the ECJ to state that notification must become a central strut in oversight regimes.[98]

However, the IPT is also shrouded in secrecy, making its efficacy and vigilance hard to discern and one is left with correlating output.[99] Up to 2013, the IPT had only upheld 0.5 per cent of alleged infringements.[100] In 2015, 77 per cent of complaints were ruled as 'frivolous or vexatious' or led to a 'no determination' outcome.[101] At the same time, the Tribunal was not aided by the frequent Government tactic of neither confirming nor denying that an individual was subject to Government surveillance,[102] leading Amnesty International to proclaim that proceedings at the IPT could descend into 'pure farce'.[103]

Prima facie, the UK's regime lacked transparency, independence, impartiality, resourcing, efficacy and efficiency. Whilst in the past, human rights bodies had affirmed the UK's safeguards,[104] it is unclear whether it would do so now having regard to contemporary jurisprudence, such as in *Szabó* and *Watson*,[105] leading the Special Rapporteur on privacy to label them 'a joke'.[106] Certainly, one may infer from the Snowden revelations that the UK system was 'limited' and nurtured function-creep and insufficient scrutiny.[107]

IPA mechanisms

With the introduction of the IPA, the UK looked to consolidate and expand its surveillance powers[108] and update its 'unworkable' oversight mechanisms replacing them with an 'independent oversight' structure.[109] This structure replaces the aforementioned Commissioners with a single Investigatory Powers Commissioner,[110] which will be an office comprised of judges having held high judicial office auditing and investigating use of all the investigatory powers under the IPA.[111]

With the advent of the Commissioner there is the creation of a new 'double-lock' ex ante authorisation for bulk powers, giving the UK something akin to quasi-judicial authorisation[112] that will involve human rights testing of any warrant approved by a minister in a judicial review style. However, this memorandum asserts that this double-lock may descend into a rubber-stamping exercise with the standard of testing expressly limited to that of a court in judicial review coupled with the presence of an elected official's prior approval potentially creating an implicit narrowing of the Commissioner's review.[113] It is to be feared, therefore, that the Commissioner will not be the independent authorisation envisaged by rights bodies;

[97] *Liberty and others v GCHQ and others (No.2)* [2015] UKIPTrib 13_77-H; *Belhaj and others v Security Service and others* [2015] UKIPTrib 13_132-H; *Liberty and others v GCHQ and others (No.3)* [2015] UKIPTrib 13_77-H-2.
[98] *Watson*, op cit, para 100.
[99] Commissioner for Council of Europe, op cit, 14.
[100] Ibid, para 12.
[101] Ibid.
[102] Ibid, para 15.
[103] Omtzigt, op cit, 20.
[104] For example, see *Kennedy*, op cit.
[105] Report of the Special Rapporteur on privacy (2016), op cit, para 39.
[106] Adam Alexander, 'Digital Surveillance "worse than Orwell," says new UN Privacy Chief' (The Guardian London, 24 August 2015), at URL <https://www.theguardian.com/world/2015/aug/24/we-need-geneva-convention-for-the-internet-says-new-un-privacy-chief> (accessed 20 March 2017).
[107] Brown, op cit, 32.
[108] Ewen MacAskill, 'Extreme surveillance becomes UK law with barely a whimper' (The Guardian London, 19 November 2016), at URL <https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper> (accessed 4 March 2017).
[109] Joint Committee on Human Rights, op cit, 5 and 7.
[110] Ibid, 29.
[111] Investigatory Powers Act 2016, Part 8.
[112] Commissioner for Council of Europe, op cit, para 27.
[113] Investigatory Powers Act 2016, sections 89(2) (communications data), 140(2) (bulk interception warrants), 159(2) (bulk acquisition warrants) and 208(2) (bulk-personal-dataset warrants).

less an adversarial civil liberties based testing of warrants and more a bureaucratic exercise in quality control.[114]

Once more, the Prime Minister will also appoint members of the Commissioner to their post, retaining the unnecessary potential compromising of independence from RIPA when appointment independent of the executive would be more appropriate.[115] Further, whilst the Commissioners provide ex ante authorisation of a kind, they will also be required to conduct ex post review, again, as the Council Of Europe have suggested it is more appropriate in terms of efficacy and transparency for two separate bodies to undertake ex ante and ex post review respectively.[116]

The role of the IPT remains largely unchanged save for the addition of a right of appeal on a point of law,[117] which is of questionable use if 77 per cent of cases (as for 2015) appear undermined by the Government's neither confirm nor deny approach, and the findings of claims as vexatious.

The UK's *evolution* therefore seems a soft one. On its face, it seems to improve transparency and oversight,[118] but the dual-lock system seems 'cumbersome' and contrived to maintain a status quo which contributed to the failings exposed in 2013.[119] Outside of oversight, the IPA retains bulk powers[120] and the power to require service providers to retain data on customers,[121] potentially prima facie contrary to contemporary regional policy standards mentioned earlier. The UK's bulk practices, as well as its oversight efficiency, will be tested in up-coming ECtHR jurisprudence.[122]

The United States

The USA has more of a streamlined ex ante judicial configuration in juxtaposition to the UK. Surveillance requests must be affirmed through the Foreign Intelligence Surveillance Court (FISC), established under the Foreign Intelligence Surveillance Act 1978 (FISA).[123] The court's primary function is one of 'gatekeeper' to surveillance requests under FISA (for external surveillance) and the USA Patriot Act (USPA) (for internal surveillance).[124] In its life, FISC has approved two bulk gathering programmes: one concerning Internet data;[125] the other telephony data.[126] The question, in keeping with this memorandum, is how did unconstitutional readings of FISA and USPA occur?[127]

---

[114] Commissioner for Council of Europe, op cit, para 30.
[115] Investigatory Powers Act 2016, section 227(1)(a)-(b).
[116] Commissioner for Council of Europe, op cit, paras 24 and 27-31.
[117] Investigatory Powers Act 2016, section 242.
[118] David Anderson QC, 'The Investigatory Powers Act 2016 – an exercise in democracy' (3 December 2016), at URL <https://terrorismlegislationreviewer.independent.gov.uk/the-investigatory-powers-act-2016-an-exercise-in-democracy/> (accessed 5 March 2017).
[119] Ibid.
[120] Investigatory Powers Act 2016, Parts 6 and 7.
[121] Investigatory Powers Act 2016, Part 4.
[122] *Big Brother Watch and others v United Kingdom* App no.58170/13 (Application communication 9 January 2014); *Bureau of Investigative Journalism and Alice Ross v United Kingdom*, ECtHR App No. 24960/15 (application communicated 5 January 2015); *10 Human Rights Organisations and others v United Kingdom* ECtHR App No. 24960/15 (application communicated 24 November 2015); Liberty, 'The People vs the Snooper's Charter: Liberty launches crowdfunded legal challenge to indiscriminate state spying powers in Investigatory Powers Act' (Liberty, 10 January 2017), at URL <https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/people-vs-snoopers%E2%80%99-charter-liberty-launches-crowdfunded-legal> (accessed 4 March 2017).
[123] Foreign Intelligence Surveillance Act 1978, section 1803.
[124] USA Patriot Act 2001.
[125] Foreign Intelligence Surveillance Act, section 702.
[126] USA Patriot Act 2001, section 215; Emily Berman, 'Quasi-Constitutional Protections and Government Surveillance' (2016) 3 *Brigham Young University Law Review* 771, 782-783.
[127] *Klayman v Obama*, 957 F.Supp 2d 1 (2013) , para 37.

Once more, as with the UK, one finds common ingredients that led to an ineffective oversight body:[128] the first being a lack of transparency; together with a lack of competing views in the ex ante approval process. FISC proceedings are held in secret,[129] and up until 2015 there was no mechanism for adversarial testing of applications.[130] The 'adversary system' is the engine for truth, yet FISC judges heard no competing views outside of the executive's arguments,[131] fanning claims that FISC was a 'rubber-stamp' with Government applications having a near perfect 99.97 per cent success rate.[132]

This could be a simple case of legal economics dictating a small chance the executive would file applications with a low chance of approval.[133] However, such arguments are undermined due to a lack of public scrutiny of 'undesirable developments in the law'.[134] This lack of public scrutiny was compounded by another ingredient, that of limited rights of appeal to the Foreign Intelligence Surveillance Court of Review (FISCR), only being available to service providers subject to data provision orders sanctioned by FISC which was utilised just once up until summer 2016.[135] This is a troubling facet of FISC as appeals promote 'decisional accuracy' and external testing of judgments.[136]

This leaves critics with having to correlate the effects of FISC. What can be correlated is a 99.97 per cent executive win rate and the decisions of other US courts challenging the legality of FISC approved programmes, such as *ACLU*,[137] *Klayman*[138] and *Riley*[139] which found FISC interpretations had gone 'far beyond' what Congress envisaged.[140] FISC itself was stated to have recognised what it was approving in these bulk-schemes were 'exceptionally broad' powers of questionable necessity,[141] but sought to avoid a confrontation with the Government it knew it 'could not win'.[142]

Prima facie, once more we find a pattern in a supposedly independent judicial ex ante oversight body of obfuscation, secrecy, untested rationales through lack of adversarial proceedings and appeals, compromised independence and a critical lack of evolution to match developing technology. However, FISC's failures were not all its own. It was forced to take on roles it was ill-suited to decide on (the legality of entire governmental surveillance endeavours) as opposed to simply gate keeping on warrant applications as it was mandated to under FISA.[143]

Some evolution has begun under the USA Freedom Act (USAFA) with Congress taking the step of clarifying telephony collection powers in the USPA,[144] limiting the ability to request data from service providers to instances where there was 'reasonable, articulable suspicion' of serious crime or national security threats relating to an 'individual, account, or personal

[128] Emily Berman, 'The Two Faces of the Foreign Intelligence Surveillance Court' (2016) 91(4) *Indiana Law Journal* 1191, 1192; Berman, op cit, 774.
[129] Rules of Procedure for the Foreign Intelligence Surveillance Court 50 U.S.C. § 1803(g), Rule 17(b).
[130] Berman, op cit, 1202.
[131] Ibid, 1203.
[132] Connor Clarke, 'Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate' (2014) 66 *Stanford Law Review* 125, 1979-2013.
[133] Clarke, op cit, 128.
[134] Berman, op cit, 1204.
[135] Ibid, 1202.
[136] *Salve Regina College v Russell*, 499 U.S. 225, 232 (1991).
[137] *ACLU v Clapper* Fed. R. App. P. 43 (2014).
[138] *Klayman*, op cit.
[139] *Riley v California*, 134 S.Ct. 2473 (2014).
[140] Andrew Crocker, 'EFF Case Analysis: Appeals Court Rules NSA Phone Records Dragnet is Illegal' (EFF, 9 May 2015), at URL <https://www.eff.org/deeplinks/2015/05/eff-case-analysis-appeals-court-rules-nsa-phone-records-dragent-illegal> (accessed 24 February 2017).
[141] *In Re* [REDACTED], *No. PR/TT* [REDACTED], *Opinion and Order*, FISA Ct. July 14 2004, paras 23 and 48; Berman, op cit, 784-785.
[142] Berman, op cit, 775.
[143] Ibid, 1239.
[144] USA Freedom Act 2015.

device'.[145] It also focussed on reforming FISC, as the body that now seemed to be affirming executive interpretations of Congressional wording.[146]

However, rather like the evolution in the UK, the expected transformations can be described as 'negligible'.[147] Section 401 USAFA introduces an adversarial ex ante element through a special advocate to FISC who may intervene as an amicus curiae. However, this power is a discretionary one held by presiding FISC judges when they feel that a 'novel' or 'significant' legal issue is under consideration, and the appointment is necessary.[148] Early evidence casts doubts as to whether this will remedy the lack of adversarial testing. Judges in *Re Tangible Things*[149] and *Re Call Detail*[150] declined to appoint an amicus even though these decisions represented new interpretations of USPA post-USAFA and were arguably novel and significant. The idea that an amicus will only be appointed in the most difficult of cases undermines the entire premise of an adversarial system.[151] Improved rights of appeal follow a similar discretionary pattern; FISC judges required to certify for review to FISCR questions of law they *decide* warrant review in the interests of uniformity or justice.[152]

A far more comprehensive protection of necessity and proportionality would have entailed not only a self-activated special advocate, but the provision of a right for that advocate to request appeal on a FISC determination.[153] With *ACLU* and *Klayman* illustrating the value of normative adversarial proceedings,[154] it is disappointing to find a neutered evolution that reads more like an abutment to an existing regime. Worryingly, in one of the few decisions published since USAFA enactment, *Re Call Detail*,[155] we find a status quo affirming *aggressive* reading of FISA which accepted a weak government argument for obtaining call records 'second hop;' potentially leading to the metadata of thousands of individuals being collected.[156]

Knowledge of *Re Call Detail* was made possible by section 402 USAFA which does attempt to increase transparency by establishing a 'declassification review' of each FISC decision where a significant judicial construction of the law is present.[157] However, this is, again, discretionary and cloaks a balancing exercise between intelligence gathering secrecy and transparency,[158] with section 402(a)(2) permitting the Director of National Intelligence to vitiate any declassification to 'protect national security'.[159] An exception that precedent suggests will swallow the discretion to publish.[160]

---

[145] Ibid, section 501; Rainey Reitman, 'The New USA Freedom Act: A Step in the Right Direction, but More Must Be Done' (EFF, 30 April 2015), at URL <https://www.eff.org/deeplinks/2015/04/new-usa-freedom-act-step-right-direction-more-must-be-done> (accessed 24 February 2017).
[146] Reitman, op cit.
[147] Berman, op cit, 1242.
[148] USA Freedom Act, section 401.
[149] *In Re Applications of the Federal Bureau of Investigation for Orders Requiring the Production of Tangible Things*, Nos. BR 15-77, 15-78, FISA Ct. June 17 2015 (2015) , paras 5-6.
[150] *In Re Application of the Federal Bureau of Investigation for Orders Requiring the Production of Call Detail Records* [REDACTED] Memorandum Opinion, FISA Ct. December 31 2015 (2015).
[151] Berman, op cit, 1243.
[152] USA Freedom Act, section 401.
[153] Berman, op cit, 1246.
[154] Ibid, 1239.
[155] *Re Call Detail*, op cit.
[156] David Greene, 'First FISC Phone Records Rulings Post-USA FREEDOM Exposes Shortcomings of Reforms' (EFF, 28 April 2016), at URL <https://www.eff.org/deeplinks/2016/04/first-fisc-phone-records-ruling-post-usa-freedom-exposes-shortcomings-reforms> (accessed 24 February 2017).
[157] USA Freedom Act, section 402; Berman, op cit, 1247.
[158] Berman, op cit, 1247.
[159] USA Freedom Act, section 402(a)(2).
[160] Berman, op cit, 1247.

Prima facie, once more it has to be concluded the USAFA, as with the IPA, is a 'small step' or a 'down-payment'[161] for future broader reform, one that would encompass the establishment of 'strong accountability and oversight mechanisms'.[162] However, the new transparency that publicised *Re Call Detail* does shed light on how the mass surveillance regime was able to runaway through aggressive interpretations by authorisation bodies concealed from public scrutiny.[163] Therefore, what can be gained from the IPA and USAFA stems from the transparency of declassification and ex ante authorisation. This allows for an 'evolved' discussion on oversight that the international community should seize with the insulated systems of the UK and the USA providing prima facie evidence for some of the main causes of contemporary mass surveillance maladies.[164]

The private sphere

Oversight attaches to a State's domestic and foreign mass surveillance programmes, but what cannot be ignored is the pervasive and ever-growing role of the private sector with regard to data storing to which such oversight does not extend.[165] The private sector's contemporary trend of 'commodification' of personal data means that a massive honey-pot of data is correlated by private firms.[166] This private phenomenon has a two-tier slant as, firstly, enabling State surveillance and, secondly, being rights-infringing of its own accord if, following *Watson*, the fact of gathering and retention is an affront to individual rights.

In the first instance, private companies find themselves aiding the State surveillance regime sometimes 'unknowingly' where States penetrate their databases,[167] sometimes 'reluctantly' where States force them to hand over consumer data, and sometimes 'willingly'[168] where a symbiotic relationship occurs between a private company's revenue generating purposes and a State's surveillance purposes. States latch onto private companies in a parasitic nature with State requests for consumer data increasing year upon year.[169] Though at least here, a State oversight regime may be engaged.

This means the vertical State-based regimes become complimented by horizontal private structures creating an interdependency across a multiplicity of providers, particularly telecommunication, website and social media providers.[170]

However, in the second instance, these providers themselves have global reach over billions of people, for example eight digital providers dominate 51 countries across the world in Europe, the US, the Middle-East and Central Asia.[171] Private communications providers frequently employ terms of service or privacy policies setting out their rights to access, edit,

---

[161] Dan Froomkin, 'USA Freedom Act: Small Step for Post-Snowden Reform, Giant Leap for Congress' (The Intercept, 2 June 2015), at URL <https://theintercept.com/2015/06/02/one-small-step-toward-post-snowden-surveillance-reform-one-giant-step-congress> (accessed 24 February 2017).
[162] Cindy Cohn and Rainey Reitman, 'USA Freedom Act Passes: What We Celebrate, What We Mourn, and Where We Go From Here' (EFF, 2 June 2015), at URL <https://www.eff.org/deeplinks/2015/05/usa-freedom-act-passes-what-we-celebrate-what-we-mourn-and-where-we-go-here> (accessed 24 February 2017).
[163] OHCHR report, op cit, para 14.
[164] Report of the Special Rapporteur on Privacy (2017) , para 30.
[165] Report of the Special Rapporteur on freedom of expression, op cit, para 1.
[166] Report of the Special Rapporteur on privacy (2016) , para 9.
[167] Report of the Special Rapporteur on freedom of expression, op cit, para 60.
[168] Arne Hintz, 'Outsourcing Surveillance-Privatising Policy: Communications Regulation by Commercial Intermediaries' (2014) 2(2) *Birkbeck Law Review* 349.
[169] Emily Taylor, 'The Privatisation of Human Rights: Illusions of Consent, Automation and Neutrality' (2016) 24 *Global Commission on Internet Governance* 1, 9, highlighting a 22% increased in requests for data from Facebook from 2013 to 2014; Dave Neal, 'Facebook transparency report show 13 per cent increase in demands' (The Inquirer, 29 April 2016), at URL <www.theinquirer.net/inquirer/news/2456584/facebook-transparency-report-shows-13-per-cent-increase-in-demands> (accessed 29 March 2017), highlighting a 13% rise in government requests for data from 2015 to 2016.
[170] Hintz, op cit, 351.
[171] Taylor, op cit, 6; those providers being Facebook, Google, YouTube, Google. Local, Wikipedia, Yahoo, Amazon, and Twitter (with the exclusion of Amazon in the Middle-East and Central Asia).

delete and share their user's data.[172] Google, YouTube, Facebook, Yahoo and Twitter not only lack clear deletion policies but reserve the right to share data with States and advertisers, as well as reserving the right to access private chat and emails. This in itself raises a host of rights questions involving,[173] inter alia, privacy, free expression and more acutely journalistic sources and privileged correspondence; the interception of which requires overriding necessity and regulation.[174]

Therefore, private mass data gathering itself raises issues of an implementation gap in terms of oversight and IHRL principles, with private firms not directly required to respect IHRL principles and ensure necessity and proportionality.[175] Instead, disparate global or regional consumer laws must be relied upon, but jurisdiction clauses in terms of service mean these providers gain 'home field advantage' in terms of the legal system a dispute will be heard in, potentially in itself deterring consumers to bring action.[176]

The question therefore becomes: should private-firms have the same responsibilities as public authorities?[177] One avenue for imposing rights standards on private firms would be through pressure on States arising out of their positive obligations under IHRL.[178] However, one need only look at the slow crawl of progression by States on their own surveillance and the fact States have become reliant on the private sector for a great deal of their surveillance, without having to actually confer any public-powers to those bodies, to realise States will likely adopt a passive approach to the issue unless forced to change the private environment.[179]

The Ruggie Principles are frequently brought up as a framework that may be buttressed to coerce more rights affirming practices from private companies.[180] The Principles reaffirm States must ensure not only public organs but also businesses under their jurisdiction respect human rights.[181] However, these Principles are non-binding and do not have the same weight as the IHRL they compliment and, despite their endorsement by the Human Rights Council, Council of Europe and Internet firms in the Silicon Valley Standard,[182] there is little evidence that the culture and practices of big tech firms are overly impacted by them.[183]

Essentially, the current accountability systems for private firms rely on public relations pressure,[184] commercial impacts from adverse public reactions to their activities, and self-initiated rectitude behaviour. However, there is evidence of prefigurative action from big tech firms which marry with Ruggie Principles such as due diligence to address potential rights impacts,[185] and transparency-focus which can act as a distress signal of sorts for the wider rights community of governmental interference in particular.[186] Firms such as Google and Facebook have been publishing transparency reports detailing their interactions with

[172] Ibid.
[173] Ibid, 6-7 .
[174] *Goodwin v United Kingdom* (1996) 22 EHRR 123 (journalistic sources requiring overriding public interest for legal interception); *Belhaj*, op cit (privileged correspondence interception requiring stringent regulatory regime).
[175] Taylor, op cit, 8.
[176] Ibid, 9.
[177] Report of the Special Rapporteur on freedom of expression, op cit, para 2.
[178] Ibid, para 8.
[179] Taylor, op cit. 3.
[180] OHCHR, 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework' HR/PUB/11/04 (2011), at URL <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf> (accessed 29 March 2017).
[181] Report of the Special Rapporteur on freedom of expression, op cit, para 9.
[182] Silicon Valley Human Rights Conference, 'Silicon Valley Standard' (2011), at URL <https://s3.amazonaws.com/access.3cdn.net/d9369de5fc7d7dc661_k3m6i2tbd.pdf> (accessed 29 March 2017), para 14.
[183] Taylor, op cit, 3.
[184] Ibid.
[185] Guiding Principles, op cit, Chapter II A 17.
[186] Ibid, Chapter II B 21.

governments creating self-managing protections which are buttressed by a contemporary proliferation of big tech firms offering increasingly sophisticated anonymisation tools to users.[187] This trend looks set to continue with tech firms taking judicial action to allow for greater transparency in their interactions with State agencies,[188] and the Ruggie Principles appear to have been something of a launch pad for civil society initiatives such as the 'Corporate Accountability Index' in 2015 that correlated data on big-tech firms and ranked them with regard to their human-rights protections,[189] finding Google to be the most rights-affirming with an aggregate 65 per cent commitment to rights protection.[190]

There seems no simple solution to the problem of privatised surveillance, but a combination of coercing States under their positive obligations, the encouragement of continued prefigurative action, and the continued engagement with civil society actors to create standards and oversight for private data retention seems the most fruitful, particularly pressuring the firms themselves who are coming under acute public pressure with 74 per cent of 23,000 Internet users surveyed expressing concerns at private surveillance and data selling.[191] Further, engagement with civil society must continue, recognising the reality that States may not be overly keen to neuter what is an important part of their surveillance regime.[192]

Conclusions and recommendations

The well-documented scope of rights intrusions of mass surveillance and data retention is the product of a runaway State machine, the handbrake of current oversight mechanisms proving inadequate leading to access and analysis of personal data without authorisation and supervision that properly accounted for necessity and proportionality.[193] All the while, further propellant was provided by a private industry which unknowingly, reluctantly or willingly fuelled this machine.[194] The case analyses above highlight how insular oversight systems, lacking adversarial testing, independence, impartiality, resourcing and being concealed from public scrutiny provided a fertile ground for function-creep and evolution prevention.

The Special Rapporteur on privacy has begun a process of staging International Intelligence Oversight Forums to correlate international information and produce results based on the realities of global oversight, with oversight regarded as the most promising avenue for effective rights protections.[195] This memorandum asserts that an international blueprint for effective oversight should be compiled, having in mind contemporary jurisprudence outlined above, the General Assembly's recommendations,[196] and the failures of two of the more sophisticated oversight regimes that led to function-creep and disproportionate surveillance and data gathering activities. In this sense, the views of the Council of Europe should be endorsed and the international community's focus should be on producing an International Intelligence Codex.[197] This Codex should not only finally settle the question of bulk power permissibility in conjunction with ECtHR and ECJ jurisprudence, but also establish the criteria for a State enacting its surveillance or data-gathering powers confining them to that

[187] Hintz, op cit, 360, 365.
[188] *In Re Motion To Disclose Aggregate Data Regarding FISA Orders*, Misc 13-04 (2013).
[189] Report of the Special Rapporteur on freedom of expression, op cit, para 14.
[190] Ranking Digital Rights, 'Corporate Accountability Index' (2015), at URL <https://rankingdigitalrights.org/index2015/> (accessed 29 March 2017).
[191] Centre for International Governance Innovation and Ipsos, 'Global Survey on Internet Security and Trust' (2014), at URL <https://www.cigionline.org/sites/default/files/documents/internet-survey-2014-factum.pdf> (accessed 29 March 2017).
[192] Report of the Special Rapporteur on freedom of expression, op cit, para 57.
[193] Report of the Special Rapporteur on privacy (2017) , para 25.
[194] Hintz, op cit, 349.
[195] Report of the Special Rapporteur on privacy (2017) , para 3.
[196] UNGA Res 68/167 (2014), para 4(d).
[197] Omtzigt, op cit, 30.

which is strictly necessary,[198] as well as prohibiting States from forcing digital communication providers from retaining data. Most importantly, this Codex should establish a clear and concise blueprint on the form that oversight bodies should take and their functions.

To that end, the following recommendations are made:

1. Internationalised standardisation of terms of language needs to be reached when dealing with governmental powers discussed here,[199] and there needs to be enshrined in Codex form recognition that rights infringement begins when data is first gathered.
2. Oversight mechanisms should always include a judicial body that provides the first ex ante authorisation of a request from an agency for surveillance powers. This should consist of individuals who have held high judicial office, being appointed independently of the executive, and having security of tenure and other forms of protection against external interference and undue influence.
3. This ex ante process would greatly benefit from a self-activating public advocate who would provide adversarial testing of the necessity and proportionality of requests from agencies as well as having the power to request an expedited appeal process from the original court decision.
4. Oversight mechanisms should always include ex post review of programmes, even where ex ante approval is provided for. However, this must be performed by a separate body to that discussed in (2), being preferably a judicial or quasi-judicial body that once more is appointed independently of the executive, and having security of tenure.
5. Both ex ante and ex post scrutiny should clearly acknowledge the irrefutable rights-impacts of the regimes they are scrutinising and the human rights triple test of legality, necessity and proportionality should be at the heart of their decisions.
6. Decisions of oversight bodies should be publicised, unless absolutely impracticable for national security reasons.
7. Focused parliamentary scrutiny should apply to the effectiveness of the work of the bodies outlined in (2) and (4) to create a layered approach to oversight protection and ensure that oversight constructs keep pace with developing technologies.
8. States must ensure adequate resourcing to these bodies, as well as ensure they are truly independent and impartial with no executive powers to distort their work.
9. The issue of private company data-gathering should come to the fore of international debate encouraging in-house evolution, transparency and engagement with civil society who can provide some oversight on domestic private data retention.

[198] Ibid.
[199] Report of the Special Rapporteur on privacy (2017), op cit, para 30.