Protection by Judicial Oversight, or an Oversight in Protection?
Matthew White*

1. Introduction

Communications data (or traffic data[1]) has been regarded as the 'who (e.g. David Smith), where (e.g. outside Parliament Square), when (e.g. 21:00 BST) and how (e.g. via hotmail.com through a browser or app) of a communication (e.g. e-mail message)'[2] and is seen as a vital tool used to investigate crime, protect the public and safeguard national security.[3] Under European Union (EU) law, the relevant definitions of traffic and location data can be found under Articles 2(b) and (c) of Directive 2002/58/EC (e-Privacy Directive). They are described as 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof' and 'any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service' respectively.

In 2006, Directive 2006/24/EC (Data Retention Directive (DRD)) was adopted with the aim of harmonising Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks (including Internet Service Providers (ISPs)),[4] to retain certain data which were generated or processed by them. Data processed or generated to be retained were through the use of landline phones, fax machines, mobile phones, and the internet[5] with the aim of ensuring that data was available for the purpose of the investigation, detection and prosecution of serious crime. In essence, the DRD allowed for the retention of data, which is described as 'a method of data preservation over a certain period of time which is thus available for retroactive investigations into electronic communications by competent authorities.'[6] According to Boehm and Cole and the Directive's preamble, the DRD was mainly created in reaction to

---

* PhD Candidate, Sheffield Hallam University. This article develops arguments made in a presentation at the 2016 Winchester Conference on Trust, Risk, Information and the Law. The overall theme for the Conference was 'Information is Power.' I would like to thank Jamie Grace for first suggesting to present at the Conference. I would also like to thank Alan Reid, James Marson, as well as Jamie for their helpful commentary on earlier drafts. I would also like to thank the anonymous reviewer for their valuable and constructive view. Finally, I would also like to thank Marion Oswald and Helen James for their support in preparing this paper for publication. All errors are my own.

[1] Advocate General Saugmandsgaard Øe uses it synonymously in Joined Cases C‑203/15 and C‑698/15 *Tele2 Sverige AB and Watson* [2016]; See Executive Summary of Privacy International and EDRi, 'Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention', (15 September 2004), <http://www.statewatch.org/news/2004/sep/data-retention.htm> accessed 29 September 2016.

[2] Home Office, 'Communications data' (17 March 2015) < https://www.gov.uk/government/collections/communications-data> accessed 29 September 2016.

[3] ibid; see also Commission of the European Communities, Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, COM (2005) 438 Final September 2005, section 1.2.

[4] Chris Jones & Ben Hayes, 'The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy' SECILE (December 2013), <http://www.statewatch.org/news/2013/dec/secile-data-retention-directive-in-europe-a-case-study.pdf > accessed 29 September 2016, p4.

[5] ibid.

[6] Kristina Irion, 'Accountability unchained: Bulk Data Retention, Preemptive Surveillance, and Transatlantic Data Protection' in Marc Rotenberg, Julia Horwitz and Jeramie Scott (eds), *Privacy in the Modern Age The Search for Solutions* (New Press 2015), 80, n6.

the terrorist attacks in Madrid on 11 March 2004 and London on 7 July 2005.[7] However, law enforcement agencies had been seeking data retention legislation some time before the 9/11 attacks.[8]

The DRD was passed despite pleas from Privacy International (PI), the European Digital Rights Initiative (EDRi), 90 NGOs and 80 telecommunications service providers to Members of the European Parliament (MEPs) to reject its passing.[9] PI and EDRi *et al* highlighted amongst other things, the illegality of data retention in light of Article 8 (the right to respect for private and family life, home and correspondence) of the European Convention on Human Rights (ECHR).[10] This raises the fundamental question of where the balance[11] should be struck between states' objectives of fighting serious crime and terrorism, and fundamental rights. The term 'fundamental rights' is used in this context because data retention is much more than issues concerning just privacy,[12] but is beyond the ambit of this article to consider other Convention Rights. The European Court of Human Rights (ECtHR), in *Klass v Germany* was conscious of the 'danger such a law poses of undermining or even destroying democracy on the ground of defending it.'[13] This issue becomes more pertinent considering the revelations made by Edward Snowden of the mass surveillance conducted by states.[14]

The DRD was met with several legal challenges, with the first being an unsuccessful challenge to its legal basis.[15] However, at a domestic level, challenges were met with greater success, with Bulgaria's Supreme Administrative Court,[16] the Romanian,[17] German Federal,[18] Czech Republic[19] Constitutional Courts and the Supreme Court of Cyprus[20] all declaring national implementation of the DRD either invalid or unconstitutional (in some or all regards) and incompatible with Article 8 ECHR.

The legality of the DRD came before the Court of Justice of the European Union (CJEU) in *Digital Rights Ireland*,[21] and before invalidating it (for incompatibility with the Charter of Fundamental Rights (CFR)), the CJEU placed great emphasis on independent/judicial authorisation of access to traffic and location data. Considering that the UK used its presidency of the EU Council to impose the DRD,[22] it was the first Member State to have a

---

[7] Preamble, para. (10), Directive 2006/24/EC; see also Franziska Boehm & Mark.D Cole, 'Data Retention after the Judgement of the Court of Justice of the European Union' (30 June 2014), < http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf> accessed 29 September 2016, p10.

[8] Chris Jones & Ben Hayes (n4), p6.

[9] ibid, p9; Privacy International and EDRi. (n1).

[10] Privacy International and EDRi (n1), section 3.

[11] Stephen Uglow, 'The Human Rights Act 1998: Part 4: covert surveillance and the European Convention on Human Rights,' Criminal Law Review [1999] 287, 288.

[12] Paul Bernal, 'Data gathering, surveillance and human rights: recasting the debate,' (2016) 1:2 Journal of Cyber Policy 243, 252-260.

[13] *Klass v Germany* App no. 5029/71 (ECHR, 6 September 1978), [49].

[14] Zygmunt Bauman et al, 'After Snowden: Rethinking the Impact of Surveillance,' (2014) 8:2 International Political Sociology 121.

[15] Case C-301/06 *Ireland v Parliament and Council* [2009] ECR I-00593, [83-84] and [92-94].

[16] Decision of the Bulgarian Supreme Administrative Court of 11 December 2008.

[17] Romania Constitutional Court DECISION no.12581 from 8 October 2009.

[18] BVerfG, judgment of the First Senate of 02 March 2010 - 1 BvR 256/08 - Rn. (1-345).

[19] The Czech Republic Constitutional Court 2011/03/22 - Pl. ÚS 24/10.

[20] Cyprus Supreme Court (Civil applications 65/2009, 78/2009, 82/2009 and 15/2010-22/2010).

[21] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECR I-238.

[22] Chris Jones & Ben Hayes, (n4), p9.

national challenge post *Digital Rights Ireland*. It was also the UK's Court of Appeal (CoA) that made a preliminary reference to the CJEU. Therefore, it is also important to consider data retention and access from a UK perspective because subsequent challenges may shape EU law affecting the other 27 Member States and it may also shape UK law irrespective of whether it decides to fully withdraw its membership of the EU. When it came to the UK's High Court (HC)[23] and CoA's[24] interpretation of *Digital Rights Ireland* in *Davis*, they differed on whether this scheme of independent/judicial authorisation was a mandatory requirement, which the lack of had already been regarded as the greatest weakness in the UK scheme of surveillance.[25] The Advocate General (AG) subsequently favoured the HC's interpretation,[26] thus ruling that judicial/independent control for access communications data should be mandatory. Prior to this, when the UK's (draft) Investigatory Powers Bill (dIPB) was introduced, it was regarded as having a 'world-leading oversight regime'[27] as it included (for the first time in the UK), a judicial element to the authorisation of interception. There is now also a judicial element to data retention notices in the Investigatory Powers Act 2016 (IPA 2016). It is welcomed that there is a growing trend towards requiring independent/judicial[28] authorised surveillance practice; however, this fundamentally overlooks addressing the axiomatic[29] and serious interference of data retention, an oversight in protection.

This article contributes to the discussion on oversight of electronic surveillance, with a focus on ECHR, UK and EU law. It presents an argument based on the ECtHR jurisprudence and the AG's Opinion in *Tele2 and Watson*,[30] that data retention is a form of secret surveillance, which poses just as serious of an interference as interception and therefore, should have equivalent safeguards i.e. that surveillance be both individually targeted on the basis of reasonable suspicion and independently-authorised in order to be demonstrably proportionate. Currently, unlike interception and access to communications data, data retention is not targeted at individuals,[31] and therefore it is submitted that transferring the power of retention to a judge would create another oversight in protection, because at present, only independence of the authorising body could be guaranteed, therefore requiring other safeguards. If the present power of data retention vested in the executive was transferred to a

---

[23] *Davis & Ors, R (on the application of) v Secretary of State for the Home Department & Ors* [2015] EWHC 2092.
[24] *Secretary of State for the Home Department v Davis MP & Ors* [2015] EWCA Civ 1185.
[25] Stephen Uglow, (n11), p296.
[26] Joined Cases C‑203/15 and C‑698/15 *Tele2 Sverige AB and Watson* [2016] Opinion of Saugmandsgaard Øe [226].
[27] Theresa May. 'Home Secretary: Publication of the draft Investigatory Powers Bill' (4 November 2015) <https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill> accessed 9 March 2016.
[28] Opinion of Saugmandsgaard Øe, (n26), [84], [86], [88], [90], [92-94], [95], [106-7], 116; *Szabo and Vissy v Hungary* App no. 37138/14 (ECHR, 12 January 2016), [77]; Home Office, 'IP Act Implementation - Programme Layer' (17 March 2017) <https://www.digitalmarketplace.service.gov.uk/digital-outcomes-and-specialists/opportunities/2158> accessed 31 March 2017.
[29] Opinion of Saugmandsgaard Øe, (n26), [254-260].
[30] ibid, [54].
[31] Though bulk interception occurs by virtue of s.8(4) of the Regulation of Investigatory Powers Act 2000 which is subject to challenge in *10 Human Rights Organisations & Others v UK* App no. 24960/15, communicated on 24 November 2015 and is currently present in Part 6, Chapter 1 of the Investigatory Powers Act 2016, furthermore there is reason to believe that this has also been conducted by several police forces - Alon Aviram, 'Revealed: Bristol's police and mass mobile phone surveillance' (10 October 2016) <https://thebristolcable.org/2016/10/imsi/> accessed 11 October 2016; Bulk acquisition of communications data has been said to occur via s.94 of the Telecommunications Act 1984 see Home Office, *Draft Investigatory Powers Bill* (Cm 9152, 2015), para 36, p 20 and via Part 6, Chapter 2 of the Investigatory Powers Act 2016.

judge, this balance would still not be struck as this too would still contravene Article 8 of the ECHR, which will be demonstrated with the UK's system of retention notice authorisation. The Grand Chamber (GC) of the ECtHR has previously held that indiscriminate data retention[32] and the automatic storage for six months of *clearly irrelevant* data cannot be justified under Article 8.[33] This is significant because the AG in *Tele2 and Watson* opined that the level of protection afforded by the CFR *must never be inferior to that guaranteed by the ECHR*.[34] Yet, the CJEU did not take this into account when it ruled in *Digital Rights Ireland*, nor does it in *Tele* 2 *and Watson*[35] and therefore, at present, this safeguard of individually targeted judicial/independent authorisation of data retention does not exist at an EU or Member State level. This article will also consider the implications for the UK following the referendum outcome of its membership of the EU.

2. Digital Rights Ireland and the move away from Kennedy v United Kingdom towards judicial authorisation:

2.1 Advocate General:

In 2010, the High Court of Ireland (HCI) requested a preliminary reference[36] to the CJEU regarding the validity of the DRD.[37] When AG Cruz Villalón gave his opinion on the matter, he criticised the EU legislature when drafting and implementing the DRD because it should have guided Member States' regulation of authorisation by *limiting* access *if not solely to judicial authorities, at least to independent authorities* and failing that making access subject to review by judicial or independent authorities on a case-by-case basis.[38]

2.2 The CJEU's Judgment:

In *Digital Rights Ireland* when the question of the DRD's validity[39] came before the CJEU, it declared it invalid.[40] One of the reasons for doing so was because '*[a]bove all*' access to the retained data was not controlled by a court or independent administrative body where the aim would be to limit access to what was strictly necessary for the purposes outlined in the DRD (Article 1(1)).[41]

In line with the AG Cruz Villalón, there was heightened concern by academics concerning the lack of judicial/independent involvement in the access to communications data. McIntyre, argued that this reasoning was significant in several regards. Firstly, it departs from the ECtHR's stance in *PG and JH*[42] by placing access to communications data on par with interception, which is welcomed considering the revealing nature of communications data.[43]

---

[32] *S and Marper v UK* App nos. 30562/04 and 30566/04 (ECHR, 4 December 2008), [125].
[33] *Roman Zakharov v Russia* App no. 47143/06 (ECHR, 4 December 2015), [225].
[34] Opinion of Saugmandsgaard Øe, (n26), [141].
[35] Joined Cases C‑203/15 and C‑698/15 *Tele2 Sverige AB and Watson* [2016].
[36] *Digital Rights Ireland Ltd -v- Minister for Communication & Ors* [2010] IEHC 221, [115].
[37] ibid, [14].
[38] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] Opinion of Cruz Villalón, [127].
[39] *Digital Rights Ireland and Seitlinger and Other* (n21), [1].
[40] ibid, [73].
[41] ibid, [62].
[42] *PG and JH v UK* App no. 44787/98 (ECHR, 25 September 2001), [42].
[43] Opinion of Saugmandsgaard Øe, (n26); *Szabo and Vissy* (n28), [53], [70]; Report of the Office of the High Commissioner for Human Rights, 'The right to privacy in the digital age' (30 June 2014), <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf> accessed 6 February 2016, para 19; see also Judge Pettiti in *Malone v UK* App no. 8691/79 (ECHR, 2 August 1984), where he noted in relation to metering (which was the then equivalent of communications data) that '*the processing of "neutral" data may be as revealing as the processing of sensitive data*.'

It also rejects the approach in *Kennedy* which praised *ex post* controls (discussed below)[44] and takes a step further than *Klass* where the ECtHR regarded judicial supervision as 'desirable.'[45] In addition it marks a return to the approach elucidated in *Popescu*,[46] *Iordachi*[47]and *Uzun*[48] where the ECtHR was of the opinion that the *body issuing authorisations for interception should be independent* and that there *must be either judicial control or control by an independent body over the issuing body's activity.* The principles of independence in *Popescu*, *Iordachi*, *Uzun* were borrowed from *Pantea v Romania*[49] and *Schiesser v. Switzerland*[50]in the ECtHR's interpretation of 'officer' in Article 5(3), the deprivation of liberty.

Furthermore, *Digital Rights Ireland* and the ECtHR cases mentioned above echo the view of Judge Pettiti in his concurring opinion in *Malone v UK*.[51] That case involved the interception of the applicant's telephone, in which the ECtHR ultimately found a violation of Article 8 because interception authorisations lacked a sufficient legal basis for the exercise of power.[52] Despite agreeing that there was a violation, Judge Pettiti believed that the majority did not delve further into the British system but he did highlight the danger threatening democratic societies in the 1980s stemming from the temptation facing public authorities to "see into" the life of the citizen. He pointed out that most Council of Europe (CoE) Member States use judicial warrants for interception similar to those used for searches of premises. It was also maintained that the governing principle of these laws was the separation of executive and judicial powers, to separate the executive initiative *and the control* of the interception. He believed had the majority decided to proceed on evaluating the British system, there would have been a violation of Article 8 for lack of judicial control, and even with detailed rules that define and delimit practices, this could still violate Article 8, again *for lack of judicial control*. He was of the opinion that judicial authorities should be left with full power of appreciation over the field of *decision and control*. This justification intensifies when comparing the factual circumstances of *Klass* (terrorism) and *Malone* (ordinary criminality) believing it was difficult to see a reason for ousting judicial control as 'at the very least such control as would secure at a later stage the right to the destruction of the product of unjustified interceptions.' It was argued that leaving the assessment of suspicion to the police alone or *even subject to the control of the Home Office* cannot be regarded as an adequate means consistent with the aim pursued, even if that aim be legitimate. This was so that in any event, practices of systematic interception of communications in the absence of impartial, independent and judicial control would be disproportionate to the aim sought to be achieved.[53]

Judge Pettiti's concerns regarding seeing into the life of citizens proved to be accurate, almost three decades before the Snowden revelations. Judge Pettiti was also of the opinion

---

[44] *Kennedy v UK* App no. 26839/05 (ECHR, 18 May 2010), [167-169]; T.J. McIntyre,'Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective.' (In: Scheinin, M., Krunke, H. and Aksenova, M. (eds.). Judges as Guardians of Constitutionalism and Human Rights. Edward Elgar, 25 November 2015) < http://ssrn.com/abstract=2694512> accessed 29 July 2016, p14.
[45] *Klass*, (n13), [55-56].
[46] *Dumitru Popescu v. Romania* App no. 71525/01 (ECHR, 26 April 2007), [71-73].
[47] *Iordachi v Moldova* App no. 25198/02 (ECHR, 10 February 2009), [40].
[48] *Uzun v Germany* App no. 35623/05 (ECHR, 2 September 2010), [72].
[49] *Pantea v Romania* App no. 33343/96 (ECHR, 3 June 2003), [238].
[50] *Schiesser v. Switzerland* App no. 7710/76 (ECHR, 4 December 1979), [31].
[51] *Malone*, (n43).
[52] ibid, [80].
[53] Stephen Uglow, (n11), p288.

that Home Secretaries should not have the power to issue interception warrants, but such power should be vested in the judiciary. This highlights two differing approaches from the ECtHR, one requiring judicial/independent control, and the other only maintaining its desirability. It will be discussed later why the former should be preferred. Although these cases concerned interception, and not the retention of, or access to communications data, it will later be argued that the same principles should apply based on the seriousness of interference with fundamental rights each pose, and the fact that all three amount to secret surveillance.

2.3 Why Judicial Control?

In 2007, the Joint Committee on Human Rights (JCHR) recommended that the Regulation of Investigatory Powers Act 2000 (RIPA 2000) should be amended to provide for judicial rather than ministerial authorisation of interceptions, or subsequent judicial authorisation in urgent cases,[54] but why? This question was posed by McIntyre, who first referred to a passage from *Klass* where the ECtHR maintained that:

> The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an *effective control* which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure.[55]

McIntyre elaborates that the need for independence reflects the conflicting incentives of the authorities which seek the measures, whom are institutionally unlikely to give adequate weight to privacy concerns, particularly in the context of terrorism where governments are prone to overreact. The judiciary, it was maintained, are most removed from the political cycle and less directly influenced by popular opinion.[56] Such pressures were noted by JUSTICE in which Ministers' may knowingly issue a disproportionate interception warrant in the hopes of obtaining the results sought.[57] This was also echoed by Baroness Hale in *Walumba Lumba v Secretary of State for the Home Department* where it was noted that:

> These are just the sort of circumstances, where both Ministers and their civil servants are under pressure to do what they may know to be wrong, in which the courts must be vigilant to ensure that their decisions are taken in accordance with the law. To borrow from the civil servants' correspondence, *the courts must be prepared to take the hit even if they are not*.[58]

Despite this, McIntyre also noted that there were significant limitations to judicial control, particularly at the initial stage of authorisation as there is a lack of an adversarial procedure. This intensifies in the national security context, where judges are removed from their expertise, often relying on one-sided claims which tend to be exploratory in nature. Despite acknowledging that specialist judges can be created (referring to the United States Foreign Intelligence Surveillance Court ("FISC")), these pose their own regulatory risks and may

---

[54] Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning* (HL 157/HC 394, 30 July 2007), 161.
[55] *Klass*, (n13), [55].
[56] ibid, n44, McIntyre, p 3.
[57] JUSTICE, 'Freedom from Suspicion Surveillance Reform for a Digital Age' (October 2011) <http://www.statewatch.org/news/2011/nov/uk-ripa-justice-freedom-from-suspicion.pdf> accessed 04 October 2016, para 84-85.
[58] *Walumba Lumba v Secretary of State for the Home Department* [2011] UKSC 12, [205].

even lose objectivity. Moreover, as surveillance becomes more technologically complex, judges would lack the specialist knowledge needed to provide adequate oversight. Therefore, McIntyre argued that judicial controls should form a wider system of accountability including specialised oversight institutions,[59] similar to what Anderson recommended (see section 4.4.4 below). This article acknowledges that the focus is primarily on judicial control, and recognises the inherent problems of a solely judicial system. Furthermore, additional personnel alongside judges in the authorisation process would not be inconsistent with European law.[60] However, this would not alter the conclusions of the article, as the body issuing the surveillance power would not be at issue (if independence is maintained), but the *manner* in which the power can be exercised.

Following McIntyre's observations, he noted that application of the principles in *Digital Rights Ireland* (which would now cover most national surveillance laws),[61] placed the requirement for prior independent review was itself a mandatory requirement under the CFR. This was irrespective of whatever other safeguards might be in place.[62] Though the DRD was invalidated, Member States still had a legal basis to impose general obligations to retain data via Article 15(1) of the e-Privacy Directive,[63] and the UK Government did just that. Therefore, the question became, would the new UK law comply with *Digital Rights Ireland*?

3. The UK's response:

The Data Retention and Investigatory Powers Act 2014:

Following the judgment in *Digital Rights Ireland*, the UK Government initially made no comment of its intentions for three months[64] and then suddenly fast tracked emergency legislation through Parliament which was then subjected to a legal challenge by Tom Watson MP and David Davis MP.[65] This emergency legislation, the Data Retention and Investigatory Powers Act 2014 (DRIPA 2014) was said to be in response to *Digital Rights Ireland*,[66] yet the concerns of *Digital Rights Ireland*, about the lack of judicial or independent oversight of access to data was not addressed in DRIPA 2014 in anyway. This issue was raised by Mr Elfyn Llwyd,[67] David Davis MP,[68] and Caroline Lucas MP.[69] Access to data continued on the basis of the public authority self-authorising process that was present in s.22(2) of the RIPA 2000. Along with access to communications data, RIPA 2000 also governs the interception of communications, which will be replaced by Part 2 and Part 3 of the IPA 2016. Therefore, case law under the ECHR (from both the ECtHR and UK) of this practice and opinions from independent UK bodies and EU/UK law on access to communications data is important as it directly impacts on the principles applicable to the retention of communications data.

---

[59] McIntyre, (n44), p 3.
[60] *Roman Zakharov*, (n33), [275]; *Digital Rights Ireland and Seitlinger and Others* (n21), [62].
[61] McIntyre, (n44), p14.; Leanne O'Donnell, 'Update on the status of data retention laws in Europe' (28 July 2015) <http://mslods.com/2015/07/28/update-on-how-the-west-is-backing-away-from-data-retention/> accessed 24 July 2016.
[62] McIntyre, (n44), p14.
[63] Opinion of Saugmandsgaard Øe, (n26), [84], [86], [88-90], [92-94], [95], [106-7], [116].
[64] Open Rights Group, 'Briefing to MPs on Data Retention Legislation' (9 July 2014) <https://www.openrightsgroup.org/ourwork/reports/briefing-to-mps-on-data-retention-legislation> accessed 13 June 2016.
[65] *Davis & Ors, R* (n23); BBC, 'Emergency surveillance law faces legal challenge by MPs' (4 June 2015) <http://www.bbc.co.uk/news/uk-politics-33000160> accessed 2 March 2016.
[66] Explanatory notes to DRIPA 2014, para 3.
[67] HC Deb 15 July 2014, vol 584, col 691.
[68] ibid, col 730.
[69] ibid, col 749.

4. Judicial authorisation of interception and access to communications data in the UK:

4.1 Case law:

Given that general obligations of data retention have been regarded as posing just as serious of an interference (*in the individual context*) as interception,[70] it is important to consider the case law on interception. In *Liberty v GCHQ*,[71] before the Investigatory Powers Tribunal (IPT), it was noted that there was no basis for objection by virtue of the absence for judicial pre-authorisation of a warrant.[72] First, the IPT noted that ECtHR did not criticise the lack of judicial authorisation in *Liberty v UK*[73]but that was mainly because the ECtHR, like in *Malone*,[74] did not concern itself with the independence of the authorisation, but with the issue of interception of external communications.[75] Moreover, the ECtHR in *Liberty v UK* found a violation *despite* there being an Interception of Communications Tribunal and the relevant Commissioner.[76] Secondly, the IPT referred to the ECtHR's judgment in *Kennedy v UK*[77]which was satisfied by the Codes of Practice, the Commissioner and the IPT itself.[78] Yet the ECtHR was not made aware at the time of the non-legally binding nature of the Codes of Practice,[79] or the broad interpretation of 'person'[80] in relation to s.8(1) RIPA 2000 interception warrants, which was contrary to the ECtHR's understanding of it relating to *one person*.[81] Moreover, the ECtHR only maintained satisfaction insofar as it related to the circumstances of the *individual case*[82] and thus left open the possibility of a contrary view considering the Snowden revelations etc.[83] Finally, the IPT referred to the case of *Telegraaf Media*[84]where the ECtHR reemphasised how impressed they were at the UK system for allowing the Interception of Communications Commissioner (IoCC) the ability to inspect all (but not the case in practice)[85] interception warrants.[86] However, as noted, the Codes of Practice are not legally binding and thus does not ensure compliance, creating uncertainty.[87]

---

[70] Opinion of Saugmandsgaard Øe, (n26), [254].
[71] *Liberty and Others v Government Communication Head Quarters and Others* [2014] UKIPTrib 13_77-H, 5 December 2014.
[72] ibid, [116(vi)].
[73] *Liberty v UK* App no. 58243/00 (ECHR, 1 July 2008).
[74] *Malone*, (n43), see Judge Pettiti's concurring opinion.
[75] *Liberty v UK* (n73), [69].
[76] ibid, [70].
[77] *Kennedy*, (n44).
[78] ibid, [158-169].
[79] See s.72(2) of RIPA 2000; In *Kennedy* (n44), the ECtHR considered s.72(1) and72(4) but not 72(2) of RIPA 2000, [26], the ECtHR considers the Code without referring to its non-legally binding nature [160-170].
[80] For example, the Secretary of State's use of the interpretation of 'person' in s.8(1) See Intelligence and Security Committee, *Privacy and Security: A modern and transparent legal framework* (2014, HC 1075) paras 42-45.
[81] *Kennedy*, (n44), [162].
[82] ibid, [169].
[83] See for example *Telegraaf* (n84) where based on *Kennedy* the Secretary of State could authorise the interception of journalist sources in violation of Article 10 and 8.
[84] *Telegraaf Media v Netherlands* App no. 39315/06 (ECHR, 22 November 2012), [98].
[85] Home Affairs Committee, *Regulation of Investigatory Powers Act 2000* (HC 2014–15, 711) para 18; Sir Anthony May, *Report of the Interception of Communications Commissioner* (HC 2015, 1113) para 6.53.
[86] The now archived Interception of Communications Code of Practice, para 4.18 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97956/interception-comms-code-practice.pdf> accessed 5 March 2016.
[87] E.g. the police are supposed to do A, but they do not have to. Under what circumstance will they not follow A? Why?

Worryingly, the IPT maintained the status quo of any interference with communications data was not as serious as interception.[88] The IPT's reasoning was based on the false analogy raised by the Respondent[89] from *Uzun v Germany*[90] that because GPS data didn't amount to the required seriousness of that of interception, the same principle applied to communications data. However, in accepting this analogy the IPT made a critical error as location data, derived from GPS *isn't* the only data that forms part of the broad definition of communications data, and in the EU context this is distinct from traffic data. Therefore, when the IPT gave weight to *Uzun* it did so by considering a case of an isolated specific type of data, which cannot be used to justify an argument that interference is less severe *whilst* ignoring the cumulative total of the different types of communications data. The IPT maintained an interpretation that interception did not require judicial authorisation, and that communications data did not pose as serious of an interference. The issue then became, would subsequent law and reports by bodies tasked with considering surveillance powers follow this interpretation?

4.2 Privacy and Security: A modern and transparent legal framework:

On 15 March 2015, the Intelligence and Security Committee (ISC) produced *Privacy and Security: A modern and transparent legal framework*,[91] a comprehensive review of the full range of intrusive capabilities available to the UK intelligence Agencies. It contains an unprecedented amount of information about those capabilities, the legal framework governing their use, and the privacy protections and safeguards that apply. When considering authorisation for interception, the ISC asked itself whether the authorisation should be determined by Ministers or judges. The Home Secretary and Sir David Omand both opined that such decisions should be left to Ministers,[92] whereas those outside Government, such as Liberty and JUSTICE's Dr Eric Metcalfe felt the power should reside with judges.[93] The ISC then considered judicial authorisation in other jurisdictions against the authorisation process in the UK and highlighted a distinct advantage they believed Ministers had over judges.[94] This advantage was that Ministers are not only more likely to be well informed of threat to national security, but are also able to take into account the wider context of the warrant application. This is later critiqued by Anderson who preferred judicial control.[95] The ISC described situations where 'there will be circumstances where it would be lawful to use intrusive powers but there may be political or diplomatic risks involved,' giving the example of the National Security Agency (NSA) intercepting Angela Merkel's phone.[96] For this reason the ISC believed that the power be left with the Minister as the judge would only assess legal compliance and therefore may *inadvertently* authorise *more* applications which are also democratically accountable.[97] However, the UK courts *have* demonstrated taking into account the wider political aspects when passing judgment.[98]

---

[88] *Liberty and Others*, (n71) [34], [111], [114].
[89] ibid, [34] and [111].
[90] *Uzun*, (n48), [66].
[91] *Privacy and Security: A modern and transparent legal framework*, (n79).
[92] ibid, para 195.
[93] ibid, paras 196-197.
[94] ibid, paras 198-202.
[95] See section 4.4.4 below.
[96] *Privacy and Security: A modern and transparent legal framework*, (n79), paras 198-202.
[97] ibid, Recommendation FF and GG, page 116.
[98] *R (Carlile) v Secretary of State for the Home Department* [2014] UKSC 60. This case concerned whether the Home Secretary had breached Article 10 of the ECHR when she refused to allow Maryam Rajavi, a "dissident Iranian politician" who had close links to Mujahedin e-Khalq, to enter the UK in order to address British parliamentarians because it would not 'be conductive to the public good.' The Home Secretary based her decision on the difficult relations over the past century and a half between Britain and Iran and the fact that

4.3 The new Acquisition and Disclosure of Communications Data Code of Practice:
The same month the ISC published their report, a new Code of Practice for the acquisition and disclosure of communications (Code of Practice) data was published. [99] A new addition to this Code of Practice was that for the first time, it required law enforcement to obtain judicial authorisation for access to communications data when intending to identify a journalist's source.[100] The use of Single Point of Contact (SPoC),[101] an accredited individual, trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs was not mandatory.[102] Furthermore, internal procedures could commence if it was believed that an immediate threat of loss of human life, such that a person's life might be endangered by the delay inherent in the process of judicial authorisation, but that the IoCC needed to be informed of this.[103] Furthermore, the new Code of Practice maintained that Designated Senior Officer's (DSO), defined in s.70(3) of the IPA 2016, as a person as a person holding office, rank or position in relation to the authority i.e. police (column 1 of Schedule 4) '*must* be independent from operations and investigations when granting authorisations or giving notices related to those operations.'[104] These were subject to exceptions in circumstances of urgency, where the public authority would not be able to call upon an independent DSO. It was submitted such circumstances *may* include:

- small specialist criminal investigation departments within public authorities which are not law enforcement or intelligence agencies; and
- public authorities which have ongoing operations or investigations immediately impacting on national security issues.[105]

Neither the IPT, the ISC nor the new Code of Practice took into account the ruling of the CJEU in *Digital Rights Ireland* with regards to judicial/independent control of access to communications data. The issue[106] raised is that that if judicial/independent authorisation is required for access to communications data which has been considered less intrusive than interception, then the logical argument would be this should also be the case for interception. Moreover, the guarantee of DSO's being independent of investigations, (which was not satisfactory in almost half of the circumstances inspected by the IoCC)[107] does not deal with the fact that the DSO is still not independent of the *organisation as a whole*.[108] Furthermore,

---

interference with Rajavi's Article 10 rights were justified as a proportionate response to national security, public safety and the rights of others which would be posed by a hostile reaction from the Iranian government and other forces in Iran. The SC held in the Home Secretary's favour by a majority of 4-1 (Lord Kerr dissenting) opining that the decision was lawful. This demonstrates that judges can and do consider, to some degree, the wider political context under the notion of proportionality [32]; See also *Miranda v Secretary of State for the Home Department & Ors* [2014] EWHC 255 (Admin), [40].

[99] Acquisition and Disclosure of Communications Data Code of Practice, (March 2015) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf> accessed 1 March 2016.

[100] ibid, para 3.78.

[101] ibid, para 3.19.

[102] ibid, para 3.24.

[103] ibid, paras 3.82-3.83.

[104] ibid, para 3.12.

[105] ibid, para 3.13.

[106] As Anderson also highlighted; see below (n118).

[107] Investigatory Powers Bill Deb 24 March 2016, col 71.

[108] Stephen Uglow, (n11), p298; LSE Policy Engagement Network, 'Briefing on the Interception Modernisation Programme' (June 2009) <http://www.lse.ac.uk/management/documents/research/research-initiatives/IMP-briefing.pdf> accessed 24 January 2017, p30.

circumstances 'may include' and therefore not limited to, would bring about an uncertain discretion to the public authority in question.

4.4 Independent Reviewer on Interception:

On June 2015, the Independent Reviewer of Terrorism Legislation David Anderson Q.C. published a well-documented report on the state of Britain's investigatory powers entitled *A Question of Trust* which set out to inform the public and political debate on these matters whilst also setting out proposals for reform.[109] On the subject of *Digital Rights Ireland*, Anderson suggested that any rules that replace DRIPA 2014, the minimum requirements for consideration should consist of 'prior authorisation by a judicial authority or independent administrative body.'[110] Anderson highlighted that judicial authorisation of interception and access to communications data was by far the most common suggestion advocated for, which he believed would be more in line with *Digital Rights Ireland*, the ECHR, and would create a greater degree of independence, as well as being be more practicable.[111]

When it came to Anderson's recommendations, recommendation 22 maintained that interception warrants should be judicially authorised by a senior or retired judge in the capacity of a Judicial Commissioner (JC).[112] Anderson's felt that although this was a radical recommendation, it was one of the easiest to arrive at.[113] Anderson's reasoning was as follows:

- The number of warrants signed by the Home Secretary and the careful consideration that each warrant required queried whether this was the best use of the Secretary of State's valuable time.[114]
- Improve public confidence.[115]
- US companies were more likely to comply with warrants authorised by a judge.[116]
- There is already an established system of judicial approval by Judicial Commissioners for other comparably intrusive measures.[117]
- ECHR jurisprudence and the implication by *Digital Rights Ireland* (as noted above) requiring approval by a court or independent body for access to communications data which Anderson considers less intrusive.[118]

Recommendation 84(e) maintained that JCs should also authorise communications data requests which are novel or contentious or which are made for the purpose of determining matters that are privileged or confidential.[119] However, when it came access to communications data in general, Anderson believed in maintaining the SPoC and giving it

---

[109] David Anderson, 'A Question of Trust, Report of the Investigatory Powers Review' (June 2015, Executive Summary) para 3,<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf> accessed 2 March 2016.
[110] ibid, para 5.76.
[111] ibid, para 12.50.
[112] ibid, para 14.47.
[113] ibid, para 14.48.
[114] ibid, para 14.49.
[115] ibid, para 14.50.
[116] ibid, para 14.51.
[117] ibid, para 14.52.
[118] ibid, para 14.53.
[119] ibid, para 14.95.

statutory footing,[120] whilst also requiring authorising DSO independence from investigations to which they authorise access to communications data.[121] Anderson recommended the removal of magisterial and shrieval approval of requests for communications data by local authorities,[122] and replacement with an Independent Surveillance and Intelligence Commission (ISIC) for authorisation.[123] This would have had the benefit of independence from higher ranking judges and the ability of drawing on expertise from different disciplines from the worlds of intelligence, computer science, technology, academia, law and the NGO sector. [124]

4.5 A Democratic Licence to Operate:

On the 15 July, the Royal United Services Institute (RUSI), the UK's leading independent think-tank on international defence and security published its independent surveillance review, having the benefit of coming after both the ISC and Anderson reviews.[125] When it came to obtaining communications data, it was recommended that relevant applications be made via the National Anti-Fraud Network (NAFN) as the national SPoC[126] with authorisation coming from the DSO.[127]With regards to interception, it was recommended that for the detection and prevention of serious organised crime, authorisation by a JC was necessary and that for national security and economic well-being purposes, the warrant should be authorised by the Secretary of State subject to a judicial review before implementation.[128]With RUSI feeling that access to communications should by authorised SPoC, it was left to the High Court to decide the matter in *Davis and Watson*.

4.6 Davis and Watson:

When the challenge to DRIPA 2014 was brought before the HC, it was interpreted that a mandatory requirement was being made when the CJEU ruled in *Digital Rights Ireland*. This requirement was that laws establishing general retention regimes *must* have provisions which expressly provide for access for restricted purposes, which *must* be dependent on prior review by a court or an administrative independent body.[129] When it came to the criticisms of the magisterial system of approval (highlighted above) it was believed they were entirely fixable, [130] therefore marking an endorsement for this judicial system. The HC said as much where they noted that the 'need for that approval to be by a judge or official *wholly independent of the force or body making the application should not*, provided the person responsible is properly trained or experienced, be particularly cumbersome.'[131]The HC was of the opinion that EU law demanded this[132] and therefore concluded that s.1 of DRIPA 2014 was inconsistent with EU law (this was one of two reasons) insofar as access to data was not made dependent on a prior review by a court or an independent administrative body[133] and

---

[120] ibid, para 14.78.
[121] ibid, paras 14.80-14.81.
[122] ibid, paras 14.82-14-83.
[123] ibid, para 14.86.
[124] ibid, para, 85, 14.99.
[125] RUSI, 'A Democratic Licence to Operate' (15 July 2015) <https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf> accessed 6 March 2016.
[126] ibid, recommendation 4.
[127] ibid, recommendation 9(3).
[128] ibid, recommendation 10(1) and 10(2).
[129] *Davis & Ors, R* (n23), [90-91(b) and (c)].
[130] ibid, [97].
[131] ibid, [98].
[132] ibid.
[133] ibid [114(b)].

made a disapplication to that effect.[134] The HC did, however, allow the Secretary of State to make an appeal to the CoA.[135]

4.7 Court of Appeal in Davis:

Before the CoA, the Secretary of State argued that the HC had interpreted *Digital Rights Ireland* incorrectly, maintaining that the CJEU was not laying down mandatory requirements for national legislation but more generally held that the DRD had failed to incorporate any safeguards that were compatible with the CFR.[136] Nor did the CFR, as the Secretary of State maintained, apply to rules concerning access of communications data by law enforcement and even if it did, nothing in *Digital Rights Ireland* suggested that the CJEU were intended to expand the CFR beyond the ECHR.[137]

The CoA believed that when the CJEU ruled in *Digital Rights Ireland*, their observations were in the context of the validity of the DRD and because national legislation may not be limited to the single objective identified in the DRD, the observations of the CJEU cannot be automatically applied to national legislation.[138] Further support, that the CoA believed that the CJEU was not laying down mandatory requirements, came from the AG's Opinion, where it was noted that he was at least, not looking for the Directive to provide detailed regulation.[139] Yet the CoA failed to mention the AG's conclusions, where it was stated that the DRD was *invalid* as a result of the *absence of sufficient regulation of the guarantees governing access* to the data collected/retained, that the DRD should be suspended until the EU legislature adopts measures necessary to remedy the invalidity, and that such measures *must* be adopted within a reasonable period.[140]

The CoA also felt that the distinctions between what the HC considered to be mandatory requirements were unsatisfactory and thus concluded that the CJEU was not laying down those requirements but were highlighting several inadequacies in the DRD.[141] The CoA also held that the HC was incorrect to conclude that DRIPA 2014 did not lay down clear and precise rules on access pursuant to a retention notice for the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such offences.[142] The CoA was correct to highlight that the CJEU was referring to the objectives of the DRD,[143] and therefore when Member States are legislating on access to communications data in the context of law enforcement, the rules need to be clear. Therefore, it was not necessary to delve into whether *Digital Rights Ireland* was limiting Member States in other contexts.[144]

When the issue of judicial/independent oversight was considered, the CoA doubted that the CJEU intended to lay down mandatory requirements in this regard because they did not refer

---

[134] ibid, [122(b)].
[135] ibid, [125].
[136] ibid, n24, [54(1)].
[137] ibid, [54(2) and (3)].
[138] ibid, [74-76].
[139] ibid, [77].
[140] Opinion of Cruz Villaló, (n38), [157-158]; For a discussion see Matthew White, 'Data retention and national law: whatever the CJEU rules, data retention may still survive!' (16 March 2016) <http://eulawanalysis.blogspot.co.uk/2016/03/data-retention-and-national-law.html> accessed 6 April 2016.
[141] *Davis MP & Ors*, (n24), [79-80].
[142] ibid, [81-82].
[143] ibid, [83].
[144] ibid, [84].

to any relevant case law nor did they consider any competing interests.[145] The CoA believed if this was the case, it would go beyond ECHR jurisprudence.[146] It highlighted that neither *Klass*[147] nor *Rotaru*[148] and importantly *Kennedy* had not gone far enough to impose a general requirement of judicial/independent approval as a necessary safeguard.[149] However, such an approach failed to highlight the ECtHR's inconsistent approach. Neither the CoA (nor the HC) mentioned *Popsecu* or *Iordachi* or *Uzun*, which stray beyond the above mentioned, only referring to *Telegraaf* as correctly maintaining that judicial approval only when it came to the surveillance of journalists.[150] *Popsecu, Iordachi* and *Uzun* all highlight that the CJEU did not in actual fact go beyond ECtHR jurisprudence as they both made the same point, just on different types of surveillance practices. The GC of the ECtHR in *Zakharov* affirmed the requirement for independence found in *Popescu*.[151] It is interesting to note that the GC referred to Secretary of State authorisations in *Kennedy* in the same paragraph, but in affirming the required independence in *Popescu* raises major doubts about any Secretary of State authorisation because they *are* part of the executive. Moreover, in *Szabo* the ECtHR when referring to the independence requirements in *Popescu*, felt that control by an independent body, normally a judge with special expertise, *should be the rule and substitute solutions the exception*, warranting close scrutiny.[152] An example of an exception could be based on Anderson's recommendation 10(1) and 10(2), national security and economic well-being purposes. The ECtHR also made express reference to *Digital Rights Ireland* (including the need for prior court/independent body review) and placed great importance on UN's Special Rapporteur recommendations (one of which included surveillance of communications must be *exclusively* under the supervision of an independent judicial authority).[153]

The ECtHR did refer to *Kennedy* and the IPT's extensive *post factum* oversight as being an example that *may* counterbalance the shortcomings of Secretary of State authorisation.[154] However, this extensive jurisdiction has received 2140 complaints from its inception (since 2000) to 2015[155] and it was only in February 2015 that the IPT found its first finding against the government.[156] From 2000 to 2015 there has been total of 16 successful complaints out of 2140, making a success rate of around 0.9%. Though *Liberty v GCHQ* was not the IPT's first finding against a public authority, it does highlight the astonishingly low success rate compared to other Tribunals.[157]

Of course, the IPT can only deal with complaints lodged, but given the number of requests for communications data, for example, the IoCC estimated 205,843 applications in 2013,[158]

---

[145] ibid, [87].
[146] ibid.
[147] *Klass*, (n13).
[148] *Rotaru v Romania* App no. 28341/95 (ECHR, 4 May 2000).
[149] *Davis MP & Ors*, (n24), [114].
[150] ibid.
[151] *Roman Zakharov*, (n33), [258].
[152] *Szabo and Vissy* (n28), [77].
[153] ibid, [23-24], [68].
[154] ibid, [77].
[155] Volume of complaints <http://www.ipt-uk.com/content.asp?id=30> accessed 23 December 2016.
[156] *Liberty & Ors v GCHQ* [2015] UKIPTrib 13_77-H; Natasha Simonsen, 'The Investigatory Powers Tribunal and the rule of law' (16 February 2015) <https://ukhumanrightsblog.com/2015/02/16/the-investigatory-powers-tribunal-and-the-rule-of-law-natasha-simonsen/> accessed 23 December 2016.
[157] JUSTICE, (n57), para 356-369.
[158] Interception of Communications Commissioner's Office, Communications Data Statistic <http://www.iocco-uk.info/docs/Relationship%20between%20applications,%20authorisations,%20notices%20and%20items%20of%20data.pdf> accessed 23 December 2016.

coupled with the fact that in the very same year the IoCC was only able to individually scrutinise 10% of law enforcement applications,[159]by way of random[160] sampling,[161]demonstrates the significant gap in which any form of independent oversight of non-independent authorisation. Although s.240(1)(a) of the IPA 2016 abolishes the IoCC, this critique highlights that this office could not have guaranteed adequate and effective control of surveillance powers.

In agreeance, Sudha Setty maintained that 'because the tribunal only acts when a complaint is brought to it, even if it were functioning in a fair and impartial manner, it is structurally unable to act as a comprehensive check on government abuse.[162]The former Chief Surveillance Inspector, Sam Lincoln noted that oversight was not rigorous enough and therefore shouldn't blame 'public authorities for exploiting opportunities that enable them to meet their operational and investigative objectives.'[163] Lincoln continues that RIPA 2000 is essentially a 'voluntary code' (this has merit considering the general savings in s.80) and the National Police Chiefs' Council lead on digital crime, Stephen Kavanagh even went as far as saying officers should sometimes 'push the boundaries' and sometimes 'go beyond what the regulations or courts accept' to protect the public.[164] The IPT has been described as a 'deeply flawed institution'[165] and even the case of *Liberty & Ors v GCHQ* in which the IPT found a breach has been severely criticised for substantially watering down the requirements set in *Kennedy*.[166]

Szabo is regarded as arguably the strongest statement by the ECtHR to date on the requirement under Article 8 for judicial authorization[167] moving away from desirability in *Klass*.[168] In his concurring opinion in *Bărbulescu v. Romania*, Judge Pinto de Albuquerque noted that in the context of employee surveillance that:

> Unconsented *collection*, access and analysis of the employee's communications, including *metadata*, may be permitted only exceptionally, with *judicial authorisation*, since employees suspected of policy breaches in disciplinary or civil proceedings must not be treated less fairly than presumed offenders in criminal procedure. *Only targeted surveillance in respect of well-founded suspicions of policy violations is*

---

[159] Home Affairs Committee, (n89).
[160] JUSTICE, (n57), para 99.
[161] Report of the Interception of Communications Commissioner, (HC 255 2015), para 7.42.
[162] Sudha Setty, 'Surveillance, Secrecy, and the Search for Meaningful Accountability' (2015) 51 Stan. J Int'l L. 69, 91; Clive Walker, Championing Local Surveillance in Counter-Terrorism, in Fergal Davis, et al., Surveillance, Counter-Terrorism and Comparative Constitutionalism 24 (2014), at 32.
[163] Sam Lincoln, 'Surveillance under RIPA: neither a strict legal framework nor rigorously overseen' (13 October 2015) <https://ukhumanrightsblog.com/2015/10/13/surveillance-under-ripa-neither-a-strict-legal-framework-nor-rigorously-overseen-sam-lincoln/> accessed 23 December 2016.
[164] Martin Bentham, 'Police 'must be given power to shut websites in child abuse and revenge porn fight'' (16 December 2016) <http://www.standard.co.uk/news/crime/police-must-be-given-power-to-shut-websites-in-child-abuse-and-revenge-porn-fight-a3422131.html> accessed 23 December 2016.
[165] Cian C. Murphy & Natasha Simonsen, 'Interception, Authorisation and Redress in the Draft Investigatory Powers Bill' (5 November 2015) <https://ukhumanrightsblog.com/2015/11/05/interception-authorisation-and-redress-in-the-draft-investigatory-powers-bill/> accessed 23 December 2016.
[166] Natasha Simonsen, (n156).
[167] Carly Nyst, 'The European Court of Human Rights Constrains Mass Surveillance (Again)' (22 January 2016) <https://www.justsecurity.org/28939/ecthr-constrains-mass-surveillance/> accessed 12 March 2016.
[168] *Klass*, (n13), [55-56].

admissible, with general, unrestricted monitoring being manifestly excessive snooping on employees.[169]

This demonstrates that even in the sphere of private surveillance (which includes collection of communications data) ECtHR judges are in favour of judicial authorisation. This falls in line with observations by Julia Hörnle, who considered the lack of *ex ante* judicial scrutiny was a deficiency which should be addressed[170] as this at best marginally satisfies the criteria for authorisation laid down in *Klass*.[171]

The reliance on *Kennedy* should not be seen as sacrosanct as 'the Court chooses the precedents it cites based on the legal issues in the case, regardless of where those cases originated.'[172] Therefore, because *Popescu*, *Iordachi*, *Uzun* and *Szabo* are all chamber judgments, just like *Kennedy*, it is argued that preference to judicial/independent control in the former cases should be followed, based on simple majority. This is given more prominence when the GC in *Zakharov* may have unwittingly undermined the independence of the authorisation process in *Kennedy*. Moreover, the ECtHR's databases of case law on HUDOC categories cases based on their importance. The 'highest level of importance being Case Reports, followed by levels 1, 2 and 3.'[173] A filtered search of 'secret surveillance' puts *Zakharov* and *Uzun* in the Case Reports category, whilst *Kennedy* and *Iordachi* are placed in level 1, and *Szabo* is placed in level 2. It must be noted that classifications of levels 1 to 3 remain provisional.[174] This demonstrates a vague indicator that *Kennedy* is not the most important case on secret surveillance measures and their authorisation mechanisms.

The CoA were mindful of jurisprudence from other Member States using *Digital Rights Ireland* as a basis for holding national legislation as invalid[175] and thus made a preliminary reference to the CJEU to clarify this matter.[176] The CoA therefore took a radically different approach which serves as comfort to the Government[177] as it preserved DRIPA 2014 whilst not providing obstacles to the dIPB.

4.8 Investigatory Powers Act 2016:

On 4 November 2015, the then Home Secretary, Theresa May announced the dIPB to Parliament.[178] May maintained that the dIPB amongst other things would establish a 'world-leading oversight regime'[179] in the form of an independent Investigatory Powers Commissioner (IPC). The IPC would consist of a senior judge, supported by a team of experts to hold intelligence services and law enforcement to account. After considering the

---

[169] *Bărbulescu v. Romania* App no. 61496/08 (ECHR, 12 January 2016), [13].
[170] Hörnle, J. 'How to control interception-does the UK strike the right balance?' (2010) 26:6 Computer Law & Security Review, 649, 654.
[171] Nick Taylor, 'State Surveillance and the Right to Privacy Surveillance & Society' (2016) 1(1) 66, 71; Stephen Uglow, (n11), p298; Joint Committee on Human Rights, (n54), Q28.
[172] Yonatan Lupu and Erik Voeten, 'Precedent in International Courts: A Network Analysis of Case Citations by the European Court of Human Rights' (2011), 42:2 B.J.Pol.S 413, 433.
[173] HUDOC FAQ: Frequently asked questions <http://www.echr.coe.int/Documents/HUDOC_FAQ_ENG.pdf> accessed 23 December 2016.
[174] ibid.
[175] *Davis MP & Ors* (n24), [117(3)].
[176] ibid, [118].
[177] David Anderson, 'Davis/Watson appeal' (20 November 2015) <https://terrorismlegislationreviewer.independent.gov.uk/daviswatson-appeal/> accessed 11 March 2016.
[178] Theresa May, (n27).
[179] ibid.

reviews by the ISC, RUSI and Anderson and proposed a 'double-lock' process for the most intrusive investigatory powers, in which a warrant would not come into force until it has been formally approved by a judge. This was regarded by May as 'one of the strongest authorisation regimes anywhere in the world.'[180] Anderson highlighted that the Bill went a long way 'to meet the cynics who see its vital powers as ripe for governmental abuse.'[181]

On November 29 2016, the dIPB became the IPA 2016.[182] Sections 227(1)(a) and (b) of IPA 2016 creates the JC and the IPC in which appointments would be made by the Prime Minister. This has been seen by others as indicating insufficient independence because the appointment is made by the executive,[183] though the ECtHR may consider this sufficient.[184] However, the ECtHR has also doubted independence where the executive is consulted on appointment *and* dismissal,[185] something that s.228(5) would allow the Prime Minister to do. The ECtHR in *Findlay v UK* noted that 'in order to maintain confidence in the independence and impartiality of the court, *appearances may be of importance*'[186] which in the UK would boost support for surveillance practices.[187] An alternative that was suggested by many was that JC's should be appointed by the Judicial Appointments Commission (JAC).[188]

Intercept warrants issued by the Secretary of State,[189] are considered by the JC on principles of judicial review.[190] Where the JC disagrees with the Secretary of State, the Secretary of State can appeal to the IPC.[191] Regarding obtaining communications data, s.61 and 62 gives the power to obtain communications data and under certain circumstances internet connection records (ICRs) to a DSO. Access to communications data are subject to exemptions if they are for the purposes of i.e. identifying or confirming journalistic sources requiring JC authorisation.[192]

This section has demonstrated there have been mixed views on whether there should be judicial control for interception *and* access to communications data. Against this back drop, it

---

[180] ibid.
[181] David Anderson, 'David Anderson: The Investigatory Powers Bill is still a work in progress' (2 March 2016) <http://www.telegraph.co.uk/news/uknews/law-and-order/12180439/David-Anderson-The-Investigatory-Powers-Bill-is-still-a-work-in-progress.html> accessed 29 July 2016.
[182] Daniella Lock, 'The Investigatory Powers Act: The Official Entrenchment of Far-Reaching Surveillance Powers' (30 November 2016) <https://www.justsecurity.org/35040/investigatory-powers-act-official-entrenchment-far-reaching-surveillance-powers/> accessed 22 December 2016.
[183] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, February 2016, Access Now, page 22 – para 27, Big Brother Watch, page 155, Bingham Centre for the Rule of Law, page 163 – para 14, <http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf> accessed 9 March 2016; Byron Karemba, 'The Investigatory Powers Bill: Putting the Investigatory Powers Commissioner in Focus (Part II)' (15 April 2016) <https://ukconstitutionallaw.org/2016/04/15/byron-karemba-the-investigatory-powers-bill-putting-the-investigatory-powers-commissioner-in-focus-part-ii/> accessed 6 May 2016.
[184] *Roman Zakharov*, (n33), [278].
[185] ibid, [279].
[186] *Findlay v UK* App no. 22107/93 (ECHR, 25 January 1997), [76].
[187] Will Dahlgreen, 'Judicial oversight gives surveillance bill public support' (15 November 2015) <https://yougov.co.uk/news/2015/11/15/judicial-oversight-surveillance-support/> accessed 5 October 2016.
[188] Joint Committee on the Draft Investigatory Powers Bill (n183), The Bar Council, page 97 - para 20, Big Brother Watch page 155, Interception of Communications Office, page 678, JUSTICE, page 710, Cian C. Murphy and Natasha Simonsen page 1016-1017 – para 5, Privacy International, page 1139 - para 156.
[189] Section 19 of the IPA 2016.
[190] Section 23(1) and (2)(a) of the IPA 2016.
[191] Section 23(5) of the IPA 2016.
[192] Section 61(3)(e) and s.77 of the IPA 2016.

is important to consider the AG's Opinion in section 5 as the Government were acting on assumption that the CJEU in *Digital Rights Ireland* were not imposing mandatory requirements. If the AG opined that judicial/independent control was a mandatory requirement for access to communications data, then this would logically mean the JC authorisation should not be limited to for e.g. identifying journalistic sources. It would also be difficult for Member States (such as the UK) to justify not having the same requirement for interception.

5. Mandatory judicial oversight?

5.1 Advocate General Saugmandsgaard Øe

On July 19 2016 the AG Saugmandsgaard Øe handed down his Opinion in the case of C-203/15 and C-698/15 (*Tele2 and Watson*).[193] The case concerned two preliminary references made by the Swedish and UK national courts on matters of data retention.[194] The AG quickly highlighted that general data retention obligations were within the scope of EU law.[195] The principal issue at hand was, as referred to by the CoA, whether the CJEU was laying down mandatory requirements, (particularly judicial/independent control of access to communications data) of EU law to which national legislation must comply.[196] The AG highlighted two opposing views.[197] The first, that the safeguards were mandatory.[198] The other, they were merely illustrative, because the CJEU gave an overall assessment of the safeguards absent, and none taken in isolation could be regarded as mandatory. In support of the illustrative view, the German Government suggested the metaphor of 'communicating vessels': a more flexible approach to one of the three aspects identified by the Court (such as access to the retained data) may be compensated by a stricter approach to the other two aspects (the retention period and the security and protection of the data).[199]

However, the AG rejected the 'communicating vessels' approach and felt that *all* of the safeguards highlighted by the CJEU in *Digital Rights Ireland* should be regarded as mandatory.[200] The AG gave several reasons for this:

- The CJEU's reasoning did not allow any possibility for a flexible approach to one of the three aspects (access, retention, data protection/security of data) to compensate for a stricter approach to the remaining two;[201]
- A 'communicating vessels' approach would deprive the safeguards described by the CJEU of any practical effect, such that individuals data whom has been retained would no longer have sufficient guarantees to effectively protect their personal data against the risks of abuse;[202]
- Implementation of these safeguards pose little practical difficulties for Member States who wish to impose general data retention obligations.[203]

---

[193] Opinion of Saugmandsgaard Øe, (n26).
[194] ibid, [5].
[195] ibid, [86-95].
[196] ibid, [59-60].
[197] ibid, [218].
[198] ibid, [219].
[199] ibid, [219-220].
[200] ibid, [221].
[201] ibid, [222].
[202] ibid, [224].
[203] ibid, [227].

The AG also pointed specifically to *Szabo* as an indicator that independent/judicial control was mandatory.[204] On the specifics of prior independent review[205] it was felt that there was no reason to take a flexible attitude to this requirement, pointing the severity of the interference posed by data retention and criticisms made by the United Nations of 'self-authorisation' systems.[206]The AG felt that prior independent review was necessary so that particularly sensitive data (i.e. professional privilege, identifying journalistic sources) may be dealt with on a case-by-case basis and all the more necessary where it is technically difficult to exclude all data from generalised retention.[207] The AG highlighted the fact that none of the three parties concerned (law enforcement, service provider, or individual) are in a position to carry out an effective review of access to retained data and therefore, intervention by an independent body becomes *imperative*.[208] The AG did highlight that in *specific* situations of extreme urgency, where making an application to the independent body would be incompatible with the situation, it would be permissible to bypass prior independent but that a swift *ex post facto* is a must.[209] Interestingly, in the same vein, the AG did also indicate that as far as possible, prior authorisation should be maintained and an emergency procedure introduced within the independent authority *in order to deal with this type of request for access*.[210] This would therefore limit the discretion of self-authorisation to be the exception, and not the rule[211] even within urgent situations.

The AG also highlighted that in *Digital Rights Ireland*, the CJEU established that service providers are under an obligation to retain data within the EU in order to facilitate the review, required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security.[212] Although, this Opinion is not binding, and it will be for the CJEU to be the final arbiter on the matter, it is clear that the AG's Opinion squares with that of the HC's in *Davis and Watson* and would therefore require any provisions in the IPA 2016 that require access to communications data be sanctioned by an judicial or independent body.

5.2 Court of Justice:

On 21 December 2016, the Grand Chamber of the CJEU handed down its judgment in *Tele2 and Watson*.[213] Just as AG Saugmandsgaard Øe articulated, the CJEU ruled that data retention was in the cope of EU law.[214] On the issue of the appropriate mechanisms for access to communications data, the CJEU affirmed the AG, and referring to *Szabo* in noting that:

> In order to ensure, in practice, that those conditions are fully respected, it is *essential* that access of the competent national authorities to retained data should, *as a general rule*, except in cases of validly established urgency, be subject to a prior review carried out either *by a court or by an independent administrative body*…[215]

---

[204] ibid, [226].
[205] ibid, [232].
[206] ibid, [234].
[207] ibid, [235].
[208] ibid, [236].
[209] ibid, [237].
[210] ibid.
[211] *Szabo and Vissy* (n28), [77].
[212] Opinion of Saugmandsgaard Øe, (n26), [238].
[213] Joined Cases C‑203/15 and C‑698/15 *Tele2 Sverige AB and Watson* [2016].
[214] ibid, [73-81].
[215] ibid, [120], [125], [134(2)].

Though this did not specifically rule these were mandatory requirements,[216] Open Rights Group regarded this part of the judgment as fully endorsing the HC in *Davis* and as serving a blow to the current DSO system.[217] This would ultimately lead to the Part 3 of the IPA 2016 having to be modified. The most likely scenario would be allowing all access to communications data to be approved by the JCs.

On the issue of data retention, the CJEU ruled that Article 15(1) of the e-Privacy Directive, read in light of Articles 7, 8, 11 and 52(1) of the CFR precludes national legislation for the purpose of fighting crime 'for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.'[218] In addition to this, the CJEU indicated that data retention measures should only be pursued when there is link or indirect link with serious criminal offences and contribute one way or another to fighting serious crime or preventing a serious risk to public security.[219] This as Graham Smith has noted 'purposes for which data may be retained which go beyond fighting serious crime, are unlikely to pass the court's muster.'[220]This was met with many positive responses as a blow to UK surveillance laws.[221] Though, Woods has argued that 'the Court [did not] expressly hold that mass surveillance was per se unlawful, so the question still remains.'[222] What the CJEU did regard as permissible, was the 'targeted' retention of data.[223]In ruling that the catch all type of data retention is not permissible under EU law, the CJEU would have made unlawful, the power in the draft Communications Data Bill[224] that was subsequently dropped, whether this affects the power in the IPA 2016 will be assessed in section 7.

6. Brexit:

On 23 June 2016, the UK voted in favour of leaving the EU,[225] and with that, concerns about how UK courts will adjudicate cases involving EU law in the immediate future have arisen.[226] However, when it comes to the issue of data protection, privacy and surveillance it

---

[216] Lorna Woods, 'Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)' (21 December 2016) <http://eulawanalysis.blogspot.co.uk/2016/12/data-retention-and-national-law-ecj.html> accessed 22 December 2016.
[217] Javier Ruiz, 'EU Court slams UK data retention surveillance regime' (21 December 2016) <https://www.openrightsgroup.org/blog/2016/eu-court-slams-uk-data-retention-surveillance-regime> accessed 22 December 2016.
[218] *Tele2 Sverige AB and Watson*, (n213), [112].
[219] ibid, [111].
[220] Julia Fioretti, 'EU court says mass data retention illegal' (21 December 2016) <http://uk.reuters.com/article/uk-eu-court-privacy-idUKKBN14A0YD> accessed 22 December 2016.
[221] Javier Ruiz, (n218); Owen Bowcott, 'EU's highest court delivers blow to UK snooper's charter' (21 December 2016) <https://www.theguardian.com/law/2016/dec/21/eus-highest-court-delivers-blow-to-uk-snoopers-charter?CMP=share_btn_tw> accessed 22 December 2016; Nicole Kobe, 'Blow for Snoopers Charter as EU court bans mass data collection' (21 December 2016) <http://www.itpro.co.uk/public-sector/snoopers-charter/27819/blow-for-snoopers-charter-as-eu-court-bans-mass-data-collection> accessed 22 December 2016; Liberty, 'Government IS breaking the law by collecting everyone's internet and call data and accessing it with no independent sign-off and no suspicion of serious crime' (21 December 2016) <https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/government-breaking-law-collecting-everyones-internet-and-call> accessed 22 December 2016.
[222] Lorna Woods, (n216).
[223] *Tele2 Sverige AB and Watson*, (n213), [108].
[224] Matthew White, (n140).
[225] House of Commons Library, 'Brexit: what happens next?' (30 June 2016) <http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7632> accessed 25 July 2016.
[226] Christina Lienen, 'Brexit and the Domestic Judiciary: Some Preliminary Thoughts on the Aftermath of Triggering Article 50' U.K. Const. L. Blog (21st July 2016)

has been pointed out that '[i]f Britain leaves the EU it will find it must still comply with European Union laws governing personal data handling and privacy anyway.'[227] In *Schrems* the CJEU ruled that in light of the CFR, Member State data protection authorities are not prevented from examining claims concerning the protection of his rights and freedoms in regard to the processing of personal data which has been transferred to a *third country* when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.[228] This has been construed as requiring almost identical degrees of protection in the third country that has data transferred.[229] In *Tele2 and Watson*, the AG highlighted that was no reason to attenuate the requirement, that since, if data is retained outside the EU, the level of protection offered by the e-Privacy Directive and the CFR cannot be ensured for persons whose data are retained.[230]However, the CJEU has since ruled that any such data retention should be occur *within* the EU.[231] On 2 October 2016, PM May announced in her first Conservative Party Conference Speech, a Great Repeal Bill.[232] PM May maintained that this would repeal the European Communities Act 1972 (ECA 1972) which would give Parliament the freedom 'to amend, repeal and improve any law it chooses.' This has been regarded as an empty gesture as 'repealing the ECA post-Brexit is legally unnecessary.'[233] If this were not the case, the UK would risk being prevented from processing personal data of EU citizens, making national data retention laws very problematic. Peter Shaar, the former German federal commissioner for data security, in a similar vein has maintained that unless 'specific arrangements on data protection are made between the EU and the UK, the United Kingdom will be seen from the EU perspective as a regular third country.'[234] Shaar continued that 'any transfer of personal data will be permissible only if the data controller and the data processor comply with the conditions laid down in the [General Data Protection Regulation],'[235] a position the House of Lord European Union Committee agrees with.[236]

Furthermore, it has even been suggested that post Brexit arrangements could lead to challenges on the basis that such arrangements violate fundamental rights under EU law, for

---

<https://ukconstitutionallaw.org/2016/07/21/christina-lienen-brexit-and-the-domestic-judiciary-some-preliminary-thoughts-on-the-aftermath-of-triggering-article-50/. accessed 25 July 2016.

[227] Steve Peers,'How would Brexit affect data protection, privacy and surveillance laws in Britain?' (5 May 2016) <https://theconversation.com/how-would-brexit-affect-data-protection-privacy-and-surveillance-laws-in-britain-57995> accessed 25 July 2016.

[228] Case C‑362/14 *Schrems* [2015], [107].

[229] Steve Peers, 'The party's over: EU data protection law after the Schrems Safe Harbour judgment' (7 October 2015) <https://eulawanalysis.blogspot.co.uk/2015/10/the-partys-over-eu-data-protection-law.html> accessed 25 July 2016.

[230] Opinion of Saugmandsgaard Øe, (n26), [240].

[231] *Tele2 Sverige AB and Watson*, (n213), [122].

[232] Theresa May, 'Prime Minister: Britain after Brexit: A Vision of a Global Britain The Prime Minister' (2 October 2016) <http://press.conservatives.com/post/151239411635/prime-minister-britain-after-brexit-a-vision-of> accessed 5 October 2016.

[233] Mark Elliott, 'Theresa May's "Great Repeal Bill": Some preliminary thoughts' (3 October 2016) < https://publiclawforeveryone.com/2016/10/02/theresa-mays-great-repeal-bill-some-preliminary-thoughts/> accessed 5 October 2016.

[234] Peter Shaar, 'Brexit and Data Protection: Out Is Out' (29 June 2016) <https://www.eaid-berlin.de/?p=1207> accessed 11 October 2016; see also Anya Proops, 'Brexit & the Future of Data Protection Revisited' (28 June 2016) < https://panopticonblog.com/2016/06/28/brexit-future-data-protection-revisited/> accessed 12 October 2016; see also Christopher Knight, 'Brexit and the GDPR – the Government Speaks' (6 July 2016) <https://panopticonblog.com/2016/07/06/brexit-gdpr-government-speaks/> accessed 12 October 2016.

[235] Shaar, (n234).

[236] European Union Committee, *Brexit: future UK-EU security and police cooperation* (HL 2016-17, 77) para 118.

curtailing the rights of EU citizens living in the UK.[237]This could be for example, data retention laws not fully respecting *Digital Rights Ireland* and *Tele2 and Watson*. Given the CJEU's judgment in *Tele2 and Watson*, it would mean that if the UK continues with certain provisions in the IPA 2016, it would be 'likely to present a clear and present danger for the economic outlook of UK data controllers and processors.'[238] However, despite the AG's Opinion, and the CJEU's judgment seemingly raising the bar for adequate safeguards in the surveillance context, it is contended that even at an EU level, this may not be as adequate as it first appears.

7. An Oversight in Protection?

7.1 Identifying the Oversight:

In *Szabo* the ECtHR maintained that:

> 'Given the technological advances since the *Klass and Others* case, the potential interferences with *email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely*.'[239]

This article has so far outlined the move towards judicially/independently authorised surveillance practices i.e. interception and access to communications data. Regarding interception, it was once considered desirable in *Klass* but now suggested to be the default in *Szabo*.[240] Prior to this, in relation to interception, the ECtHR had already *required* this in *Popescu*, *Iordachi* and *Uzun*. There is indication to also in terms of access to communications data as Anderson concedes in light of *Digital Rights Ireland* that:

> 'It is possible however that a more independent authorisation mechanism may be required in the future.'[241]

Although the UK will be slow to react to calls for judicial authorisation[242] of any measure that was once at the hands of the Secretary of State, there are signs of compromise. It is welcomed, however slow that may be, that in the modern era that the calls for judicial authorisation should be the norm to better protect the fundamental rights the Member States are duty bound to protect. For all that is welcomed, however, there appears to be a noteworthy oversight in this debate, and that is the axiomatic interference posed by data retention itself. [243]

7.2 Judicial Treatment of Data Retention:

Judicial treatment of data retention, it is submitted, has been met with mixed and conflicting views. In *Digital Rights Ireland* the CJEU despite acknowledging that retention of data

---

[237] Ronan McCrea, 'Can a Brexit Deal Provide a Clean Break with the Court of Justice and EU Fundamental Rights Norms?' (U.K. Const. L. Blog 3 October 2016) < https://ukconstitutionallaw.org/2016/10/03/ronan-mccrea-can-a-brexit-deal-provide-a-clean-break-with-the-court-of-justice-and-eu-fundamental-rights-norms/#comment-63688> accessed 11 October 2016.

[238] Cybermatron, 'Squaring the data protection circle just got harder for the UK' (21 December 2016) <http://cybermatron.blogspot.co.uk/2016/12/squaring-data-protection-circle-just.html> accessed 29 December 2016.

[239] *Szabo and Vissy*, (n28), [53].

[240] ibid, [77].

[241] David Anderson, (n109), para 14.53.

[242] Select Committee on the Constitution, *Surveillance: Citizens and the State* (*second report*) (HL, 2008–09, 18-I) para 163.

[243] Opinion of Saugmandsgaard Øe, (n26), [254-260].

constituted a particular serious interference with rights,[244] regarded it as *genuinely satisfy[ing] an objective of general interest*.[245] Not only that, the CJEU felt that data retention did not adversely affect the essence of the fundamental rights in question.[246] The HC interpreted this as seeing no reason why the exercise of the power to retain should need prior independent approval.[247] Even counsel opposing DRIPA 2014 in that case accepted that the CJEU could not have meant communication service providers (CSPs) could only lawfully retain communications data in relation to suspects that would contribute to the prevention, detection or prosecution of serious criminal offences, such a measure the HC deemed impracticable as the CJEU was only concerned with provisions of *access*.[248]This position has merit because in the subsequent case of *Schrems*, the CJEU maintained that the legislation permitting the public authorities *to have access* on a generalised basis to the content of electronic communications must be regarded as compromising the essence of Article 7 of the CFR.[249] Ryan, however, completely disagrees and believes *Digital Rights Ireland* acted as a restraint on data retention because one of the CJEU's key criticisms was that data retention applied to all users of communication services without distinction and limitation.[250] The AG in *Tele2 and Watson* also opined in line with *Digital Rights Ireland*, that data retention did not adversely affect the essence of the right.[251] However, the AG later contradicted himself[252] by accepting that in the *individual context* a general data retention obligation would facilitate *equally serious interference* as targeted surveillance measures, *including those which intercept the content of communications*[253]something which the CJEU in *Schrems* accepted *would* adversely affect the essence of the right.[254] This creates the link between data retention and interception whereby rules regarding interception should equally apply to data retention based on the seriousness of the interference with fundamental rights.

Further evidence for the lack of consideration of data retention came about when the Anti-terrorism, Crime and Security Bill was being passed, Lord Rooker maintained that the IoCC would have a power (the assumption is of a power of auditing) in relation to data retention under Chapter II of Part I of RIPA 2000,[255] but no such power has ever existed. This makes it necessary to consider data retention from a UK perspective in section 7.3.

Judicial treatment of data retention, however, now has to be considered in light of the CJEU's judgment in *Tele2 and Watson*. Much of the praise for the CJEU's judgment fundamentally misses the purpose of the reference from Sweden, which was asking whether a 'general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime' is compatible with the CFR. The CJEU answered in the negative and so

---

[244] *Digital Rights Ireland and Seitlinger and Others*, (n21), [39].
[245] ibid, [44].
[246] ibid, [39-40].
[247] *Davis & Ors, R*, (n23), [85], [99].
[248] ibid, [70].
[249] *Schrems*, (n228), [94].
[250] Michael. H. Ryan, 'Is government access to your communications data lawful? The decision of the Divisional Court in Davis v Home Secretary' U.L.R. [2015] 20(5), 55-60.
[251] Opinion of Saugmandsgaard Øe, (n26), [155-159].
[252] Matthew White, 'The new Opinion on Data Retention: Does it protect the right to privacy?' (27 July 2016) < https://eulawanalysis.blogspot.co.uk/2016/07/the-new-opinion-on-data-retention-does.html> accessed 29 July 2016.
[253] Opinion of Saugmandsgaard Øe, (n26), [254].
[254] *Schrems*, (n228), [94].
[255] HL Deb 4 December 2001 vol 629 cols 787-826.

this would in fact prevent powers that were dropped in the draft Communications Data Bill. Clause 1 maintained that:

> **1 Power to ensure or facilitate availability of data**
>
> (1) The Secretary of State may by order—
>
> (a) *ensure that communications data is available to be obtained from telecommunications operators* by relevant public authorities in accordance with Part 2, or
>
> (b) *otherwise facilitate the availability of communications data to be so obtained from telecommunications operators.*
>
> (2) An order under this section may, in particular—
>
> (a) provide for—
>
> (i) *the obtaining (whether by collection, generation or otherwise) by telecommunications operators of communications data*,
>
> (ii) the processing, *retention* or destruction by such operators of data so obtained or other data held by such operators.

As it can be seen, clause 1 would have encompassed the type of power that would now be unlawful under EU law because it would have placed general and indiscriminate obligations on telecommunications operators, neither based on necessity or proportionality, this is even more so as the CJEU ruled that data retention should be the exception, not the rule.[256] The CJEU continued that EU law in light of the CFR does however, permit the targeted retention of traffic and location data for the purpose of fighting serious crime. This is so provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.[257] The CJEU sustained that limitations on:

> [N]ational legislation must be based on objective evidence which makes it possible to *identify a public whose data is likely to reveal a link, at least an indirect one*, with serious criminal offences, and to *contribute in one way or another to fighting serious crime or to preventing a serious risk to public security*.[258]

The CJEU gave an example of such limitation using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.[259] Section 7.3 will demonstrate why this is unlikely to affect data retention obligations in the IPA 2016.

---

[256] *Tele2 Sverige AB and Watson*, (n213), [104].
[257] ibid, [108].
[258] ibid, [111].
[259] ibid.

The CJEU were reluctant to hold that data retention adversely affected the essence of the rights because it does not permit the retention of content of communications,[260] this is despite the AG in *Tele2 and Watson* in a contradictory fashion highlighted that data retention creates an equally serious interference with rights as measures which *intercept* the *content* of communications.[261] The AG continued that the risks associated with the access to communications maybe greater than access to the content of communications.[262] This contradiction is given further weight when CJEU shared the view of the AG in this regard.[263] What is more, is that even if one were to follow the CJEU's distinction, simple research by iiNet has demonstrated that embedded data about communications like Twitter, Facebook, and websites does in fact reveal content of communications (such as tweets), and lots of it.[264] This makes the position of the CJEU in differentiating content from communications data in terms of adversely affecting the essence of more difficult to justify.

7.3 Data Retention Powers in the Investigatory Powers Act 2016, Adequate Judicial Approval?:

Now that the IPA 2016 has come into force, it is worth noting the relevant provisions of Part 4. Before considering the JC mechanism for retention, it is necessary to examine the powers granted to the Secretary of State. Section 87(1) allows the Secretary of State to issue a retention notice, requiring telecommunications operators to retain relevant communications data if it is considered necessary and proportionate for a variety of purposes mentioned in s.61(7)(a)-(j). It is at this point uncertain whether all such provisions would constitute serious crimes for EU law compliance, but s.61(7)(b) may need modification and be further defined, s.61(7)(d) would appear compatible with the *risk to public security* as maintained by the CJEU in *Tele2 and Watson*. But as the CJEU highlighted, all that is required is that an indirect link to a serious crime needs to be established to justify retention, so for example, identifying a person in s.61(7)(i) who has died could aid in the investigation of a murder or where the person is a suspected of killing someone but cannot identify themselves due to lack of capacity or memory loss. Or another example could be data retention on the grounds of protecting public health (s.61(7)(e)) with the aim of preventing the supply of drugs found in s.5(3) of the Misuse of Drugs Act 1971 (MDA 1971). Vanessa Franssen asked the question of how much leeway would Member States have when it came to the notion of 'serious crime?' Would 'the list of Eurocrimes (which are in fact broad categories of crimes) in Article 83(1) TFEU then be of sufficient guidance?'[265] It would appear that Member States would have considerable discretion in determining what constitutes a 'serious crime' provided that this satisfies proportionality, and therefore the reasons for retention in s.61(7)(a)-(j) may not be affected at all. It is interesting to note, however, that the IPA 2016, does have a definition of serious crime, found in s.263(1) which is described as anyone over 18 who commits an offence with no previous convictions could reasonably be expected to be sentenced to three years of imprisonment or more. There is also a second definition of serious crime, which can be subdivided into three aspects:

- Conduct that involves use of violence;

---

[260] ibid, [101].
[261] Opinion of Saugmandsgaard Øe, (n26), [254].
[262] ibid, [259].
[263] *Tele2 Sverige AB and Watson*, (n213), [99].
[264] iiNet, 'Protecting your privacy: Our stand against 'mandatory data retention'' (21 July 2014) <http://blog.iinet.net.au/protecting-your-privacy/> accessed 30 December 2016.
[265] Vanessa Franssen, 'The Future of National Data Retention Obligations – How to Apply Digital Rights Ireland at National Level?' (25 July 2016) <http://europeanlawblog.eu/2016/07/25/the-future-of-national-data-retention-obligations-how-to-apply-digital-rights-ireland-at-national-level/> accessed 30 December 2016.

- Conduct that results in substantial financial gain; and,
- Conduct by a large number of persons in pursuit of a common purpose.

In this regard, violence is not defined, and so broadens the scope of serious crime, as for example, the Sentencing Council recommends a maximum of 2 years' custody or unlimited fine for assault with intent to resist arrest under s.38 of the Offences against the Person Act 1861 (OAPA 1861).[266] Therefore, the three-year sentencing requirement would become redundant. The second element of serious crime, the substantial financial gain is not defined either. Is substantial financial gain relative to the person's financial situation gaining this? Or is it an arbitrary figure made on a case-by-case basis? Does it even require the substantial gain to be criminal, is it fraud or theft etc? Finally, conduct carried out by a large number of persons in pursuit of a common purpose is also substantially broad, would this include protestors as well as rioters? In any event of these criticisms, if they were added to the provisions of retention notices, this again may satisfy 'serious crime' for the purposes of *Tele2 and Watson*.

Section 87(2) details the contents of a retention notice which may:

a) relate to a particular operator or description of operators;
b) the retention of all or any description of data; and
c) the period or periods for which data is to be retained.

Section 87(2) as allows other requirements which shall not be focussed on i.e. making different provisions for different purposes etc. A reason why this provision may prove unproblematic based on *Tele2 and Watson* is that this power is more qualified than the general and indiscriminate retention of all data from all subscriber and users because the Secretary of State determines which operators and what data is to be retained and could therefore constitute 'targeted' retention. Granted it is still theoretically possible for all operators in the UK to be required to retain all data of users and subscribers, it can be argued drafting s.87(2)(a)-(b) in any other way would actually make it difficult to implement a measure the CJEU felt was permissible. This measure refers to geographical criterion, as the retention obligation cannot be determined by operator, but by location, and therefore would require a variety of operators to retain data in a given area. It could further be argued that the requirement of necessity and proportionality are a prerequisite for issuing a retention notice. Section 87(3) prevents retention for more than twelve months and therefore it is suggested that s.87(1)-(3) may already satisfy the requirements set out by the CJEU in *Tele2 and Watson*[267] and may even satisfy exceptions to the rule if grounded in necessity and proportionality.

Regarding the requirement of retention making it possible to identify 'a public,' this is not defined by the CJEU. The CJEU accepted this could constitute multiple geographical areas, which again is not defined. This therefore gives Member States enough discretion to determine for themselves just how wide these geographical areas could encompass provided they can establish there is a high risk of preparation for or commission of such offences. In the UK, crime stats revealed that in 2009/10, the risk of being a victim of any household

[266] Sentencing Council, 'Assault Definitive Guideline' (2011), <http://www.sentencingcouncil.org.uk/wp-content/uploads/Assault_definitive_guideline_-_Crown_Court.pdf> accessed 19 January 2017, p15-19.
[267] *Tele2 Sverige AB and Watson*, (n213), [108].

crime was higher in the most deprived areas.[268] The top 10% of deprived areas in the UK[269] could therefore theoretically have geographical retention notices imposed in those areas. The statistics also indicated that victims of any household crime were higher in urban areas than rural.[270] Similarly to deprived areas, it is possible to impose retention obligations in urban areas based on higher propensity for household crimes. What is classified as urban depends on what classification is used,[271] possibly increasing discretion. Statistics also revealed London was the region with the highest rates of total recorded crime, violence against the person, offences against vehicles and other theft offences. London also had a higher British Crime Survey (BCS) risk of personal crime than for England and Wales overall.[272] In addition to this it was noted that 62% of robberies in England and Wales were recorded by just three forces, the Metropolitan Police, Greater Manchester and the West Midlands, which counts for only 24% of the population. The same police forces also had 54% of the total of selected serious offences involving a knife, with a greater proportion in more urban forces.[273] These stats could be used to impose retention obligations in areas covered by these police forces. Anderson asked whether the CJEU meant that 'it could be acceptable to perform "general and indiscriminate retention" of data generated by persons living in a particular town, or housing estate, whereas it would not be acceptable to retain the data of persons living elsewhere?'[274] This is why the reference from Sweden and the answer from the CJEU becomes crucial, by making limited distinctions (i.e. not a catch all power to every operator and every subscriber and user and all data) on (which can be general and indiscriminate in their own right) data retention, it will still keep data of the vast majority who are in no way connected to serious crime,[275] where for example, the homicide rate in the UK is 10 per million population (excluding 96 cases).[276]

Section 87(4)(a) would seemingly prevent third party data retention, which has been regarded as neither necessary nor proportionate.[277] Section 87(4)(c) and (d) respectively prevent data retention notices from requiring the retention of data that is not necessary for the functioning of the system and which is not retained or used by the system operator for any other lawful purpose. It is to be noted that this new insertion only relates to an operator who provides or controls a telecommunications *system*. Section 261(10) notes that a telecommunications operator is a person who offers or provides a telecommunications service to the UK, or controls or provides a telecommunications system wholly or partly in the UK. The

---

[268] John Flatley, Chris Kershaw, Kevin Smith, Rupert Chaplin and Debbie Moon, 'Crime in England and Wales 2009/10' (July 2010), <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/116347/hosb1210.pdf> accessed 1 January 2017, p166-167.
[269] UK areas of deprivation, <https://www.ukonlinecentres.com/funding/current-funding/uk-areas-of-deprivation> accessed 1 January 2017.
[270] John Flatley, (n268), p168-171.
[271] '2001 Rural-urban classification,' <http://webarchive.nationalarchives.gov.uk/20160105160709/http://www.ons.gov.uk/ons/guide-method/geography/products/area-classifications/rural-urban-definition-and-la/index.html> accessed 1 January 2017.
[272] John Flatley, (n268), p172.
[273] ibid, p172-173.
[274] David Anderson, 'CJEU judgment in Watson' (21 December 2016) <https://terrorismlegislationreviewer.independent.gov.uk/cjeu-judgment-in-watson/> accessed 1 January 2017.
[275] Opinion of Saugmandsgaard Øe, (n26), [252].
[276] John Flatley, 'Crime in England and Wales: year ending June 2016' (20 October 2016) <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2016> accessed 1 January 2017.
[277] *Szabo and Vissy*, (n28), Concurring Opinion of Judge Pinto De Albuquerque, [6].

explanatory notes of DRIPA 2014[278] noted that telecommunication services include companies who provide internet-based services, such as webmail.[279] Therefore, the same restraints on retention in s.87(4)(c) and (d) would not apply to companies such as Facebook and Google who offer many internet based services, and has been suggested would be of greater interest to the security services in any event.[280] This omission has great significance considering that there are allegations that Google *are* indeed storing third party data. Such retention has been regarded by Peter Schaar, as possibility violating fundamental rights.[281]By not placing third party data retention constraints on telecommunications services, the UK authorities could still get access to third party data, thus potentially making s.87(4)(c) and (d) redundant.

Section 89 introduces JC approval of retention notices. It makes note that when reviewing the *conclusions* of the necessity and proportionality of the Secretary of State's decision, the JC must apply the same principles of judicial review, [282] and where the JC refuses, reasons must be given.[283] The Secretary of State can appeal to the IPC to decide whether to approve the decision to give the notice.[284]

Section 90(1) allows a telecommunications operator to refer a retention notice (as a whole or any aspect of it) back to the Secretary of State and that they are not obliged to comply with the notice until the Secretary of State makes a review.[285] Section 90(6) requires the Secretary of State to consult the Technical Advisory Board (TAB), (a body which advises the Home Secretary on whether the obligations imposed on communications service providers (CSPs) under RIPA) and a JC before deciding the review. Section 90(7) requires the TAB to consider the technical requirements and financial consequences and s.90(8) requires the JC to consider the notices' proportionality *and not their necessity*. Section 90(9) requires both the TAB and JC to give the operator an opportunity to provide evidence before reaching conclusions which they must report back to the operator and the Secretary of State. Section 90(10) allows the Secretary of State to consider the TAB and the JC's conclusions, and may vary the notices or confirm its affects, subject to the approval by the IPC.[286] This makes a change from previous drafts which essentially granted the Secretary of State the power to judge for their own cause.[287]

The IPC must consider the necessity and proportionality on judicial review principles.[288] Similarly, if the IPC refuses, reasons must be given.[289]Section 91(2)(b) requires the IPC consider matters with in a way that complies with general duties in relation to privacy found in s.2. It is beyond the scope of this article to consider s.2 but it must be noted, confining this

---

[278] Definition is replicated in the IPA 2016, subject to the removal of 'public.'
[279] Explanatory Notes to DRIPA 2014, paras 5 and 56.
[280] Rory Cellan-Jones, 'Web surveillance - who's got your data?' (2 April 2012) <http://www.bbc.co.uk/news/technology-17586605> accessed 8 October 2016.
[281] Matthias Spielkamp, 'Google's Private Data Retention' (1 July 2016) <https://mobilsicher.de/uncategorized/googles-private-data-retention> accessed 11 October 2016.
[282] Section 89(2)(a) of the IPA 2016.
[283] Section 89(3) of the IPA 2016.
[284] Section 89(4) of the IPA 2016.
[285] Section 90(4) of the IPA 2016.
[286] Section 90(11) of the IPA 2016.
[287] Previous versions, didn't require the Secretary of State to adhere to the conclusions of the TAB or even the IPC.
[288] Section 91(1) and.91(2)(a) of the IPA 2016.
[289] Section 91(3) of the IPA 2016.

issue solely to privacy risks overlooking other fundamental rights,[290] one of with the CJEU in *Tele2 and Watson* noted was freedom of expression.[291] Further, s.2 may, in any event be an empty gesture given that in s.229(7) JC's must ensure that they do not jeopardise the success of an intelligence or security operation or a law enforcement operation, compromise the safety or security of those involved, and most importantly, they must not *unduly impede the operational effectiveness* of an intelligence service, a police force, a government department or Her Majesty's force. Though this does not appear to affect the giving or modification of retention notices under s229(8)(e). Section 243(1)(c)(czb) and (czc) puts retention notices under the jurisdiction of the IPT (which brings its own concerns),[292] which are challengeable by virtue of s.243(1)(i)(ba) and s.243(2)(a)(aza) the power to quash such notice.

The issues surrounding the system of JC approval with regards to interception was discussed when written evidence was submitted to the Joint Committee on the Draft Investigatory Powers Bill. It is therefore necessary to consider the concerns raised, given that JC approval of retention notices essentially mirror that of interception. Several criticisms of the judicial review process, characterised it as being a restriction of power[293] and that judicial authorisation on application by the Secretary of State is more appropriate[294] because the JCs are unlikely to stray beyond conventional *Wednesbury* principles and therefore, currently do not 'adequately provide standards of access to justice or fairness that the rule of law requires.'[295] Furthermore, in *Baker v Secretary of State for the Home Department*[296] Information Tribunal (National Security Appeals) noted that:

(i) Judges operating judicial review principles are not second stage administrators, even in ECHR territory. Theirs is a review, not an appellate role. So a margin of judgement is to be allowed to the administrator.

(ii) The intensity of judicial supervision is always dictated by context.

(iii) This is so 'even' where ECHR rights are invoked.[297]

However, and for balance, Hickman believed that a real problem with putting decisions in the hands of judges, was that it would off-load responsibility from the public official, tempting them to adopt an attitude of 'if its good enough for the judge its good enough for me' which could lead to a protection gap.[298] This, however, does not consider that judges already approve measures that seriously interfere with fundamental rights, with such decisions

---

[290] Paul Bernal, (n12).
[291] *Tele2 Sverige AB and Watson*, (n213), [92].
[292] Privacy International, 'Judges of the Investigatory Powers Tribunal visited MI5 in 2007 for a secret briefing' (28 July 2016) <https://privacyinternational.org/node/908> accessed 29 July 2016.
[293] Joint Committee on the Draft Investigatory Powers Bill (n183), Amnesty International, page 46 – para 21, Center for Democracy & Technology, page 248 – para 10.
[294] ibid, Bingham Centre for the Rule of Law, page 164 – para 14.
[295] ibid, para 15.
[296] *Baker v Secretary of State for the Home Department* [2001] UKIT NSA2.
[297] ibid, [75].
[298] Thomas Hickman, 'The Investigatory Powers Bill: What's Hot and What's Not?' (U.K. Const. L. Blog. 11 December 2015) <https://ukconstitutionallaw.org/2015/12/11/tom-hickman-the-investigatory-powers-bill-whats-hot-and-whats-not/> accessed 8 October 2016.

themselves amenable to challenge.[299] Anderson already noted that democratic accountability in this regard is limited. [300] Hickman was also of the opinion that judicial review principles would not be limited to *Wednesbury* principles as in human rights cases, courts will decide for themselves whether a measure is necessary and proportionate which judges will surely adopt.[301]

However, Baroness Hale in *Miss Behavin' Ltd* highlighted that the role of the court in human rights adjudication is quite different to that of *judicial review*. With the former, the court is concerned with whether the human rights of the claimant have in fact been infringed, but with the latter whether the administrative decision-maker properly took them into account.[302] Although, Baroness Hale referred to instances where the HoL considered the merits of policy and legislation,[303] these were not judicial review proceedings and in *R (SB)*[304]Lord Bingham believed that the courts approach to proportionality must not be constrained by traditional judicial review, but at the same time it is not a shift to a *merits based* review.

Judge Walsh joined by judge Russo in their partly dissenting opinion in the ECtHR case of *Vilvarajah*,[305] were scathing of judicial review where it was noted that 'a national system which it is claimed provides an effective remedy for a breach of the Convention and *which excludes the competence to make a decision on the merits* cannot meet the requirements of Article 13.' Although that issue concerned the requirements of Article 13, it highlights the difference between judicial review and judicial authorisation. The six principles of judicial authorisation were summarised by Elias LJ *Mills & Anor*:[306]

1. Granting warrants must only be sought as a last resort and should not be employed where less draconian measures can achieve that objective.
2. Full and frank disclosure to the judge, even where it might prove adverse to the application.
3. Duty not to mislead a judge.
4. Granting resides with a judge who must bring a *"rigorous and critical analysis"* to the application and *satisfy himself or herself* that the material provided justifies the grant of the warrant.
5. The judge ought to give reasons for decisions made.
6. The application must not be made for an ulterior purpose.

Under the IPA 2016, the JC and IPC will only consider the *conclusions* of a decision to issue a retention notice. There is no obligation on the Secretary of State to make a full and frank disclosure and therefore, the JC and IPC could be misled[307] (accidently or deliberately) as former MI5 intelligence officer, Annie Machon maintained. This could put the JC and IPC in a position where they were unable to give a rigorous and critical analysis of a notice. In essence, the JC and IPC could be given a summary a summary of a summary of a summary

---

[299] For example, in *Rossminster Ltd* (see below).
[300] David Anderson, (n109), para 12.47.
[301] Thomas Hickman, (n298).
[302] *Belfast City Council v. Miss Behavin' Ltd (Northern Ireland)* [2007] UKHL 19, [31].
[303] ibid.
[304] *R (SB) v The Governors of Denbigh High School* [2006] 2 WLR 719, [30].
[305] *Vilvarajah and Others v UK* - App nos. 13163/87; 13164/87; 13165/87; 13447/87; 13448/87), 30/10/1991, (ECHR, 30 October 1991) [3].
[306] *Mills & Anor, R (on the application of) v Sussex Police & Anor* [2014] EWHC 2523, [26].
[307] Joint Committee on the Draft Investigatory Powers Bill, (n183), Annie Machon, para 8, p944.

of a summary of the original intelligence case.[308] An extra 'summary' was added because they consider *conclusions*. During the Public Bill Committee session on the Investigatory Powers Bill, David Anderson was asked whether the JC would receive the same evidence as the Secretary of State (regarding interception, but the same principle applies), and he responded that this would be the case having had a private assurance detailing as such.[309] However, Sara Ogilvie of Liberty was not convinced of this as such private assurance was not on the face of the legislation.[310] It must be submitted that Sara Ogilvie concerns are well founded *because* the JC and IPC only review the conclusions and unlike in cases regarding control orders where disclosure was *judicially controlled*.[311] The GC in *Zakharov* noted that it is *essential* that the supervisory body 'has access to all relevant documents, including closed materials and that all those involved in interception activities have a duty to disclose to it any material it required.'[312]

Moreover, the fourth requirement crucially requires the judge to consider the application on its *merits*, something that is precluded in judicial review. The fifth requirement is also of importance because this requires the judge to give reasons *for* allowing the application thus enabling any party affected to understand why and possibly challenge.

Due to there being no guarantee of high intensity review, nor of treating surveillance measures in the same manner as control orders, it has been suggested to drop any notion of judicial review altogether. This would remove any doubts about a merit based judicial assessment and in the absence of this, it was suggested that the Home Secretary should make clear for *Pepper v Hart* purposes, that the proper construction of the judicial review clauses is one that permits an autonomous assessment by the JCs as an alternative compromise.[313]

As McIntyre noted, there is a lack of adversarial procedure inherent in judicial authorisation,[314] this is no different for the JC system as Lord Pannick noted that the JCs will 'not hear representations by lawyers acting for the person who is to be the subject of the intrusive measure, and who will not know of the proposed surveillance.'[315]Karemba highlights Pannick's idea of 'counsel to the judiciary or special advocates to ensure a fair exploration' for each warrant sought.[316] Karemba continues that given the incorporation of judicial review principles, the JCs will not hear 'contrasting submissions on what intensity of review applies in each context.'[317] This being important as Martin Chamberlain noted that 'in practically any judicial review case, a key point of contention between the parties is where on

---

[308] ibid, para 7, p944.
[309] Investigatory Powers Bill Deb 26 March 2016, col 12.
[310] ibid, col 17.
[311] *Mohamed & Anor v Secretary of State for the Home Department* [2014] EWCA Civ 559, [44].
[312] *Roman Zakharov*, (n33), [281].
[313] Byron Karemba, 'The Investigatory Powers Bill: Introducing Judicial Authorisation of Surveillance Warrants in the United Kingdom – Putting the 'Double-Lock' in Focus (Part I),' (U.K. Const. L. Blog. 22 March 2016) <https://ukconstitutionallaw.org/2016/03/22/byron-karemba-the-investigatory-powers-bill-introducing-judicial-authorisation-of-surveillance-warrants-in-the-united-kingdom-putting-the-double-lock-in-focus-part-i/> accessed 4 March 2016.
[314] McIntyre, (n44), p3.
[315] David Pannick, 'David Pannick: Safeguards provide a fair balance on surveillance powers' (November 12 2015) <http://www.thetimes.co.uk/tto/law/article4611174.ece> accessed 18 January 2017.
[316] Byron Karemba, (n183).
[317] ibid.

the spectrum that case lies.'[318] Karemba continues that such a safeguard would be desirable by the ECHR referring to *Zakharov* where the GC noted that:

> Since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any [ex ante] review proceedings, it is *essential* that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights.[319]

In this context, it is possible to argue that this is not only desirable, but *essential*, and as Karemba highlights, is something already undertaken in immigration litigation involving "national security" concerns, with special advocates.[320] For example, the JC could be convinced that access communications data is not as serious as access to content[321] and therefore, the scope of review could be less intense. However, a special advocate could remind the JC that retention of and access to communications data is just as (if not more) serious of an interference as access to content, and therefore,[322] intensifying the review.

Section 227(7) does not achieve institutional separation between the JC and IPC as a JC can be an IPC and vice versa. Section 229(1)(b) requires the IPC to review by way of audit, inspection and investigation the *retention of communications data*. This creates a situation where it has been argued that the Government's chosen regulatory body is likely to be *investigating the consequences of its own decisions*.[323] The IoCC warned that JC's who were involved in authorisations must be operationally distinct from those that carry out *post facto* audit and oversight functions.[324] However, it is submitted that, irrespective of the IoCC views, this may fall foul of the ECHR, as this would run contrary to the principles established in *Popescu*, *Iordachi* and *Uzun* of independent authorisations subject to independent controls. Moreover, the blending of functions of the JC and IPC may be regarded as giving rise to doubts of their independence.[325]

A potential threat to JC and IPC independence can also be demonstrated by s.239(1) that allows the Secretary of State to modify their functions. Section 267(1)(a) also allows the Secretary of State and even the Treasury to modify any provision made by or enactment made under the IPA 2016 by way of statutory instrument. This includes via s.267(1)(c) the power to make supplementary, incidental, consequential, transitional, transitory or saving provisions without further explanation. The ability to alter functions of the JC and IPC has been seen as 'anathema to the idea of operational independence to ordain ill-defined power on the object of scrutiny to alter the functions of the scrutiniser.'[326] Though, through s.267(3)(e), said statutory instruments now requires approval by both Houses of Parliament by way of resolution. This can be bypassed by virtue of s.267(8) subject to an affirmative

---

[318] Joint Committee on the Draft Investigatory Powers Bill, *oral evidence*, 16 December 2015, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/oral/26441.html> accessed 18 January 2017.
[319] *Roman Zakharov*, (n33), [233].
[320] Byron Karemba, (n183).
[321] *Liberty and Others*, (n71), [34], [111], [114].
[322] *Tele2 Sverige AB and Watson*, (n213) [99].
[323] Joint Committee on the Draft Investigatory Powers Bill (n183), Amberwalk Training Limited, page 32-33 - para 15.
[324] ibid, Interception of Communications Commissioner's Office, page 683 – para 15-16.
[325] *Roman Zakharov*, (n33), [280]; *Huber v Switzerland* App no. 12794/87 (ECHR, 23 October 1990), [43]; *Brintcat v Italy* App no. 13867/88 (ECHR, 26 November 1992), [21].
[326] Byron Karemba, (n183)..

procedure, laid out in s.267(9)(a), but even this could potentially be bypassed.[327] If functions regarding retention notices could be altered, this could make the JC and IPC subordinate to the executive,[328] and therefore lacking independence for ECHR compliance.[329]

In addition to potential JC and IPC's subordination, by means of functionality control, via s.238, the Secretary of State also has the power to determine (subject to mandatory consultation with the IPC and approval by the Treasury) the staffing, accommodation, equipment, facilities and services that is to be provided for the JC's. The concern here is that it is the Secretary of State *who determines what is necessary* for the JC/IPC's to carry out its functions, and not the body that *is* carrying out the functions. This degree of control could also threaten the independence of the JC/IPC system. The system of judicially authorised data retention becomes crucial when considering the serious interference with fundamental rights they pose. This is a step in the right direction, but sections 7.6.4-7.6.6 will demonstrate why, even if the inadequacies highlighted are resolved, the judicial system for authorisation retention still would not satisfy the ECHR.

7.4 Data Retention as Serious Interferences with Fundamental Rights:

Both European courts have acknowledged the seriousness of interference posed by data retention. The CJEU in *Digital Rights Ireland* acknowledged[330]and accepted that it affected all persons and all means of electronic communication.[331] The AG in *Tele2 and Watson* also highlighted its severity.[332] Judge Pettiti in his concurring opinion in *Malone v UK* maintained that *the processing of "neutral" data may be as revealing as the processing of sensitive data*. In relation to *interception*, it was noted that that '[t]hrough use of the "mosaic"[333] technique, a complete picture can be assembled of the life-style of even the "model" citizen,' this is the same for communications data. The types of data to be retained extends beyond the types of data the CJEU may have considered because s.87(9)(b) can impose obligations to *generate* data, and thus the interference can become more severe.

7.5 Data retention as Secret Surveillance:

The protection of private life *can* more acutely be found in the ECtHR's own prior case law. The ECtHR has previously noted that e-mail and internet usage fall within the ambit of Article 8[334] and on numerous occasions has held that the *storage* of private information amounts to[335] or is akin to[336] secret surveillance. Support also comes from the CoA in *Davis* where it was highlighted that the HC distinguished the case of data retention from *Kennedy* on the 'ground that [*Kennedy*] was concerned with an individual warrant *and not mass*

---

[327] Revoking provisions (i.e. IPC and JC's functions) of the IPA 2016 via s.271(2) doesn't require Parliamentary approval by way of resolution, only an annulment because s.267(3)(a) only refers to amend or repeal, but is silent on revoking.
[328] *Nevmerzhitsky v Ukraine* App no. 54825/00 (ECHR, 5 April 2005), [125].
[329] *Roman Zakharov*, (n33), [258].
[330] *Digital Rights Ireland and Seitlinger and Others*, (n21), [39].
[331] ibid, [57].
[332] Opinion of Saugmandsgaard Øe, (n26), [254-260].
[333] 'Mosaic theory describes the concept that individual actions may not rise to the level of a search in and of itself, but may constitute a search when aggregated' See Bethany. L. Dickman, 'Untying Knotts: The Application of Mosaic Theory to GPS Surveillance in UNITED STATES V. MAYNARD' (2011) 60: 3 American University Law Review 731, n15.
[334] *Copland v UK* App no. 62617/00 (ECHR, 3 April 2007), [41].
[335] *Rotaru*, (n148), [41], [59]; *Segerstedt-Wiberg and Others v Sweden* App no. 62332/00 (ECHR, 6 June 2006), [71], [76].
[336] *S and Marper*, (n32), [99].

surveillance'[337] therefore implying data retention *is* mass surveillance. Moreover, Clarke noted that '[d]ata retention proposals...are unequivocally a weapon of mass surveillance.[338] Although data is retained by telecommunication operators, it is *de facto* held by the UK because the control[339] of such data resides within the IPA 2016 and the fact that telecommunication operators cannot disclose the existence or the contents of a retention notice,[340] save for a request by the IPT,[341] highlighting its secretive nature. Therefore, if it is contended that data retention is to be regarded as secret surveillance, and poses similar interferences as interception,[342] then, accordingly, the same safeguards should apply; control by a judge.[343] There have been calls for the retention notices to approved by a judge by the Council of Europe Commissioner for Human Rights,[344] BT and Virgin,[345] Privacy International[346] and Simon Pooley,[347] which should apply at EU level and has, been reflected in s.89 of the IPA 2016.

7.6 When a Perceived Safeguard Masks an Inherent Problem:

The introduction of judicially ordered retention notices may go some way in providing for adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance.[348] However, the Grand Chamber (GC) of the ECtHR has previously held that indiscriminate data retention[349] and the automatic storage for six months of clearly irrelevant data cannot be justified under Article 8.[350] The former case, *S and Marper v UK* concerned the retention of finger print and DNA records. The GC was struck by blanket and indiscriminate nature of the power because:

> [119] material may be *retained irrespective of the nature or gravity of the offence* with which the individual was originally suspected or of the age of the suspected offender...
> [122] Of particular concern in the present context is the risk of stigmatisation, *stemming from the fact that persons in the position of the applicants, who have not been convicted of any offence and are entitled to the presumption of innocence,* are treated in the same way as convicted persons...
> [125] In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, *fails to strike a fair balance* between the competing public and private interests and that the respondent State has *overstepped any acceptable margin of appreciation* in this

---

[337] *Davis MP & Ors*, (n24), [114].
[338] Roger Clarke, 'Data retention as mass surveillance: the need for an evaluative framework' International Data Privacy Law (2015) 5 (2): 121-132, p127.
[339] Part 3, and Part 4 of the IPA 2016.
[340] Section 95(2) of the IPA 2016.
[341] Section 243(5)(c)(ha) of the IPA 2016.
[342] Opinion of Saugmandsgaard Øe (n26), [254].
[343] *Rotaru*, (n148), [59]; *Szabo and Vissy* (n28), [79].
[344] Council of Europe Commissioner for Human Rights, 'Democratic and effective oversight of national security services' (May 2015) <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2796355&SecMode=1&DocId=2286978&Usage=2> accessed 14 March 2016, p62.
[345] Joint Committee on the Draft Investigatory Powers Bill (n183), BT, page 213 - para 23, Virgin Media, page 1323.
[346] ibid, Privacy International, page 1162 - para 284.
[347] ibid, Simon Pooley, page 1106 - para 2.4.
[348] *Roman Zakharov*, (n33), [302].
[349] *S and Marper*, (n32), [125].
[350] *Roman Zakharov*, (n33), [225].

> regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society. *This conclusion obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data*.

The findings of the GC in *S and Marper* have clear applications to the detailed information revealed about individuals' private lives by communications data.[351] Moreover, in subsequent ECtHR rulings on data retention, the Court as held that 'protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life' and 'that the *need for such safeguards is all the greater when it comes to protecting personal data subject to automatic processing, especially when these data are used for police purposes*.'[352] This would suggest that protection in relation to communications data retention should be more acute due to the automatic nature of processing data of individuals and even more so when it is for police purposes. These principles are therefore important in its application to data retention at an EU level as the AG himself noted that the CFR must never be inferior to the ECHR.[353] The GC criticised the UK regime for not distinguishing between those who had been *suspected* and those who had committed offences. Even taking into account the CJEU's ban of general and indiscriminate catch all data retention, this is still profound because suspicion would not be a necessary component for the justification of retention. As the AG indicated, most data retained is of individuals who bare *no relation* to serious crime and therefore such retention of data is clearly irrelevant. This therefore, still creates issue with the presumption of innocence to an unprecedented and unacceptable level. The 'identifiable public' the direct or indirect relationship with serious crime, and even the data and communication type, persons liable etc established by the CJEU in *Tele2 and Watson* is a much lower threshold than the verification of 'the existence of a *reasonable suspicion* against the *person* concerned' where 'there are *factual indications* for suspecting that person of planning, committing or having committed criminal acts' that may give rise to measures of secret surveillance. Section 2.2 demonstrated that the ECtHR were willing to transfer principles of independence from its interpretation of 'officer' Article 5(3) into the surveillance context. Therefore, in this regard, it is submitted that notion of 'reasonable suspicion' found in Article 5(1)(c) is also transferable given that it is a prerequisite for the adoption of any surveillance measure under the ECHR. The ECtHR have noted that 'officers' must review the circumstances mitigating for and against a measure, deciding by reference to legal criteria whether the reasons justify the measure.[354] This, in other words, means to consider the *merits* of the decision.[355] When the requirement of reasonable suspicion is not met, or the measure is unlawful, the measure must cease.[356]Reasonable suspicion requires more than suspicion held in good faith, it 'requires the existence of facts or information which would satisfy an objective observer that the person concerned may have committed the offence' which is dependent in all the circumstances.[357]

---

[351] Ian Brown, 'Communications Data Retention in an Evolving Internet' (2010) 19:2 International Journal of Law and Information Technology 95, 103.
[352] *S and Marper*, (n32), [103]; *B.B. v France* App no. 5335/06 (ECHR, 17 December 2009), [61]; *M.K. v France* App no. 19522/09 (ECHR, 18 April 2013), [35].
[353] Opinion of Saugmandsgaard Øe, (n26), [141].
[354] *Pantea*, (n49), [231]; *Schiesser*, (n50), [31].
[355] *Aquilina v Malta* App no. 25642/94 (ECHR, 29 April 1999), [47].
[356] *McKay v the United Kingdom* App no. 543/03 (ECHR, 3 October 2006), [40].
[357] *Ilgar Mammadov v Azerbaijan* App no. (ECHR, 22 May 2014), [88].

The requirements, the GC maintained also required surveillance measures to meet the requirement of 'necessary in a democratic society' including 'whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means.'[358]The CJEU's reasoning is based on the assumption that data retention is the least restrictive means, highlighted by its inability to rule that retaining communications data adversely effects the essence of the right and that it genuinely satisfies an objective of general interest. It was already argued that data retention constitutes a measure of secret surveillance, and therefore the same principles apply. The ECtHR's view accords with the House of Lords Select Committee's view of targeted surveillance, which is 'directed at particular *individuals*' unlike the CJEU's view in which the Select Committee would regard as mass surveillance.[359] Although the CJEU's idea of geographical criterions may serve to limit any catch all power, that in itself is still victim of a general and indiscriminate power based on residence. This would create another human rights issue, as the GC of the ECtHR has considered that places of residence constitute an aspect of personal status for the purposes of Article 14 (discrimination),[360] which can be used in conjunction with Article 1 Protocol 1 (property and possessions)[361] and the 'home'[362] aspect of Article 8. Baroness Hale in *Countryside Alliance* was aware of the two separate, but related fundamental values, one was 'the inviolability of the home and personal communications from official snooping.'[363] Home is established under Article 8 even with a 19-year absence provided there are sufficient continuing links for home to be considered.[364]

The most significant aspect of *S and Marper* was that the retention itself was contrary to the Convention *without* having to consider the safeguards that may have been in place i.e. judicial/independent control from an EU perspective. Despite retention notices in the IPA 2016 which would now be under the control of the JC and IPC, and notwithstanding the criticisms highlighted above, the JC and IPC could still allow retention notices that required telecommunications operators to retain *any* and *all* descriptions of data (even with geographical constraints), most being clearly irrelevant, as the AG in *Tele2 and Watson* noted.

Moreover, there are questions as to the appropriateness of the length of retention notices. In the UK, retention periods are currently 12 months, and as indicated, the ECtHR consider even half of that time period if irrelevant, to be unjustified even when it relates to *individuals*.[365] This was mistakenly interpreted by the AG in *Tele2 and Watson* as making a six-month retention period acceptable.[366] This was an issue the CJEU was silent on in *Tele2 and Watson*. This puts *Digital Rights Ireland*, the AG's Opinion and CJEU's judgment in *Tele2* and the interpretation of Article 15(1) of the e-Privacy Directive in direct contrast with the ECHR and the ECtHR's rulings, something which Recital 11 of the e-Privacy states Member States must accord with. This also raises the important issue in this particular instance as the CFR *is* inferior to the ECHR.[367] This is all the more problematic as the CJEU held that the

---

[358] *Roman Zakharov*, (n33), [260].
[359] *Surveillance: Citizens and the State*, (n242), para 24-25.
[360] *Carson v UK* App no. 42184/05 (ECHR, 16 March 2010), [79-1].
[361] ibid, [61-71].
[362] *London Borough of Harrow v. Qazi* [2003] UKHL 43, [8].
[363] *Countryside Alliance and others, R (on the application of) v Attorney General & Anor* [2007] UKHL 52, [116].
[364] *Gillow v UK* App no. 9063/80 (ECHR 24 November 1986), [46].
[365] *Roman Zakharov*, (n33), [44-48], [260].
[366] Matthew White, (n252).
[367] ibid.

interpretation of the e-Privacy Directive (and therefore Member State implementation of data retention measures) *must* be undertaken *solely* in the light of the CFR.[368] Martinico argues that the CJEU still holds the reasons connected to its interpretive monopoly dear, and betray its lack of tolerance for interpretive competitors.[369] This is also reflected in the CJEU's *Opinion 2/13* on the EU's accession to the ECHR, this affirmed *Melloni*[370] in that 'national standards of protection of fundamental rights must not compromise the level of protection provided for by the Charter or the primacy, unity and effectiveness of EU law.'[371] The CJEU noted that Article 53 of the ECHR allowed Member States to raise human rights standards beyond the ECHR, something which would compromise the CFR or primacy of EU law.[372] This of course assumes that protection by the CFR is identical in every regards to corresponding rights found within the ECHR. Observations indicated above, however, doubt this in the particular context of data retention. Therefore, a situation is created where Member States are compelled through the primacy of EU law to provide weaker protections that would not occur on a stricter interpretation of the ECHR. That, or risk violating EU law to protect Convention Rights.[373]

In his concurring opinion in *Szabo*, Judge Pinto De Albuquerque believed that mandatory third-party data retention, whereby Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law-enforcement and intelligence agency access, appeared neither necessary nor proportionate.[374] It must be noted that Judge Pinto De Albuquerque confuses data retention with third-party data retention, the latter involves for example BT retaining data concerning activity on Twitter (even if said user uses BT's services for access to the internet). If Judge Pinto De Albuquerque meant the latter, this would no longer appear permissible under the IPA 2016 (see section 7.7.3). If, however, Judge Pinto De Albuquerque meant the former (which based on his description it appears to be the case), this would clearly add to the observations above and pose serious questions on *any* obligation to retain and its compatibility with the ECHR, at Member State and EU level. Judge Pinto De Albuquerque also believed that the line between criminal justice and protection of national security was blurring significantly, and that the sharing of data between law-enforcement agencies, intelligence bodies and other State organs risked violating the right to privacy, because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another. Thus, he concluded, States should take steps to ensure that effective and independent oversight regimes and practices are in place, with attention to the right of victims to an effective remedy.[375]

Retention notices under the IPA 2016 and any general obligation to retain (whether geographically based or 'targeted') under EU law run contrary to ECHR principles, and just transferring the power to issue said notice (in the UK's case, a JC or IPC) would still not create a Convention compliant system as:

---

[368] *Tele2 Sverige AB and Watson*, (n213), [128].
[369] Giuseppe Martinico, 'Is the European Convention Going to Be 'Supreme'? A Comparative-Constitutional Overview of ECHR and EU Law before National Courts' (2012) 23:2 EJIL 401, 424.
[370] Case C‑399/11 *Stefano Melloni v Ministerio Fiscal* [2013].
[371] *Opinion 2/13*, [188].
[372] ibid, [189].
[373] Matthew White, 'A Threat to Human Rights? The new e-Privacy Regulation and some thoughts on Tele2 and Watson' (10 January 2017) <http://eulawanalysis.blogspot.co.uk/2017/01/a-threat-to-human-rights-new-e-privacy.html> accessed 11 January 2017.
[374] *Szabo and Vissy*, (n28), Concurring Opinion of Judge Pinto De Albuquerque, [6].
[375] ibid.

> '[T]he implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, *it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power*.'[376]

In this context, this virtually unfettered[377] power refers to the general and indiscriminate nature of powers exercised under a constraining power, a discriminatory indiscriminate power. Though not specifically ruling on it (instead focussing on proportionality) in *S and Marper* the GC acknowledged that it was an essential component in determining Convention compliance.[378] Using interception as a basis,[379] in *Kruslin v France* the applicant claimed that the incidental interception of his calls amounted to a violation of Article 8.[380] Despite the interception being ordered by an investigating judge, whom the ECtHR admitted was an independent authority,[381] it *still* amounted to a violation of Article 8 for not indicating with reasonable clarity the scope and manner in which public authorities could exercise their discretion.[382] This reasoning was based on the system that did not provide for adequate safeguards against various possible abuses. The ECtHR explained by way of example that the *categories of people liable* to have their telephones tapped by judicial order and the nature of the offences which may give rise to such an order were *nowhere defined*. It is suggested that this is akin to an aimless obligation to retain communications data. There were further inadequacies ranging from no upper limit on the duration of interception, circumstances in which intercepted material must be destroyed particular when an individual had been acquitted or an accusation had been discharged.[383] This squared in line with the reasoning that the judges should not have unfettered power.[384] There is no upper limit on retention at an EU level, and at a UK level, it is 12 months, as noted, even half of that time period in the individual context violates the ECHR.

In *Matheron v France*, another case involving judicially authorised interception, the French Government contended that this fact of judicially authorised interception was sufficient to establish the existence of effective control. However, the ECtHR was not convinced holding that that such reasoning would lead to the conclusion that the quality of the magistrate who orders and supervises the interception implies, *ipso facto*, the lawfulness and the conformity of the interceptions with Article 8 of the Convention. Such reasoning would make any remedy for the interested parties inoperative.[385]

In *Kopp v Switzerland*[386]Judge Pettiti felt that ECtHR case law laid down the *requirement* of supervision by judicial authorities and this grew ever more important 'in order to meet the threat posed by new technologies.' He also maintained that judicially authorised

---

[376] *Roman Zakharov*, (n33), [230].
[377] *Liberty v UK* (n73), [64].
[378] *S and Marper*, (n32), [99].
[379] Because it was already argued, by virtue of posing similar interferences as interception, similar principles should apply to data retention.
[380] *Krusliin v France* App no. 11801/85 (ECHR, 24 April 1990), [25-26].
[381] ibid, [34].
[382] ibid, [36].
[383] ibid, [35].
[384] ibid, [30].
[385] *Matheron v France* App no. 57752/00 (ECHR, 29 March 2005), [40].
[386] *Kopp v Switzerland* App no. 23224/94 (ECHR, 25 March 1998).

monitoring[387] even where having valid basis in law '*must be used for a specific purpose, not as a general "fishing"*[388] *exercise to bring in information*.' Fishing shares an analogy with data retention in that it does not target individuals.[389]

Prior to this line of case law from the ECtHR, Lord Salmon in the UK House of Lords, dissenting in *ex parte Rossminster Ltd*[390] highlighted potential issues with judicial authorisation noting that:

> 'If the judge gives that as his reason for issuing a warrant, it seems to me to follow that his reason for issuing it cannot be that he is so satisfied by the information given to him on oath by an officer of the Inland Revenue of the detailed facts which the officer has ascertained; but that the judge's reason for issuing the warrant was *because the officer had stated on oath that there is reasonable ground to suspect*...'[391]

The importance of this was that Lord Salmon highlighted that (just as the ECtHR did later) judicial authorisation must be effective in practice.

Moving back to the IPA 2016, if retention notices were under the control of the JC and IPC, and s.89 still applied, they would not be able to notify individuals[392] that their rights had been infringed (as it has been argued current data retention notices violate the ECHR) due to s.231 i.e. notifying individuals of serious errors or in the public interest. Sections 231(2) and (3) indicate that errors are only considered serious if they cause significant prejudice or harm and finding a violation of the ECHR is not sufficient for an error to be considered serious. However, in *Vidal Hall* the HC held that where Article 8 is engaged, and for any breach of that right, a person has a right to an effective remedy,[393] which would not be possible under s.231, thus creating Article 13 ECHR issues, a right to an effective remedy. However, Article 13 is not incorporated through the Human Rights Act 1998 (HRA 1998). On the other hand, the CFR has a similar right, that being Article 47 which stipulates that '[e]veryone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article…'[394] The CoA in *Vidal Hall* referred to *Benkharbouche*[395] and that:

> '[I]n so far as a provision of national law conflicts with the requirement for an effective remedy in article 47, the domestic courts can and must disapply the conflicting provision; and (v) the only exception to (iv) is that the court may be required to apply a conflicting domestic provision where the court would otherwise have to redesign the fabric of the legislative scheme.'[396]

---

[387] Hal Roberts and John Palfrey, 'The EU Data Retention Directive in an Era of Internet Surveillance' in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (MIT Press, 2010) 617, p35.
[388] Stephen Uglow, (n11), p289.
[389] Franziska Boehm and Paul de Hert, *The rights of notification after surveillance is over: ready for recognition?* (Yearbook of the Digital Enlightenment Forum, IOS Press 2012), pp. 19-39.
[390] *R. v Inland Revenue Commissioners ex parte Rossminster Ltd* [1980] A.C. 952.
[391] ibid, 1019.
[392] *Roman Zakharov*, (n33), [287]; Franziska Boehm and Paul de Hert, 'Notification, an important safeguard against the improper use of surveillance - finally recognized in case law and EU law' (2012) 3:3 European Journal of Law and Technology <http://ejlt.org/article/view/155/264> accessed 29 March 2017.
[393] *Vidal -Hall & Ors v Google Inc* [2014] EWHC 13 (QB), [110].
[394] *Google Inc v Vidal-Hall & Ors* [2015] EWCA Civ 311, [96].
[395] *Benkharbouche & Anor v Embassy of the Republic of Sudan (Rev 1)* [2015] EWCA Civ 33.
[396] *Google Inc v Vidal-Hall & Ors*, (n394), [98].

In *Vidal Hall*, the CoA disapplied s.13(2) of the Data Protection Act 1998 (DPA) as the consequence of this 'would be that compensation would be recoverable under section 13(1) for *any* damage suffered as a result of a contravention by a data controller of any of the requirements of the DPA'[397] and therefore no legislative choices were made by the court. With regards to error reporting in the IPA 2016, s.231(2) and (3) would have to be disapplied as non-material damage or non-pecuniary loss are covered by both Article 23 of the Data Protection Directive (DPD) and Article 8 of the ECHR.[398] Moreover, s.231(4)(a) compels the IPC to consider the seriousness of the error and its *effect* on the person. This may be seen as further restriction on the notification of errors, as individuals are rarely aware they are under surveillance. The CoA in *Vidal Hall* was of the opinion that '[i]t is the distressing invasion of privacy which must be taken to be the primary form of damage (commonly referred to in the European context as "moral damage") and the data subject should have an effective remedy in respect of that damage'[399] which may serve as broadening the interpretation of s.231(4) i.e. data retention itself engages Article 8. Knowing that retention notices can be served on any given number of telecommunications operators may cause the requisite distress because the conduct of the individual is not related to the interference or invasion of privacy and other fundamental rights.

However, disapplying s.231(2) and (3) may have the benefit of allowing the IPC to notify individuals anytime that their Article 8 rights have been breached, but it will create the problem of also compelling the IPC to notify *every* individual whose data is subject to a retention notice and not under suspicion, in reality the vast majority. This may have the knock-on effect of an increase in number of claims to the IPT, therefore the problem still resides with the power to issue retention notices. As noted, national legislation cannot be disapplied for lack of an effective remedy if doing so would redesign the fabric of the legislative scheme. Disapplication of the retention notice regime may do just that. Therefore, having not incorporated Article 13 of the ECHR into domestic law, and Article 47 of the CFR potentially not being effective, it may be before the ECtHR where this issue would have to be resolved especially considering post Brexit judicial apprehension.[400] Although the CJEU has ruled that:

> [T]the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities seemingly.[401]

This, however, only deals with notification of access to data and not the retention of.[402] This section has demonstrated that both at an EU, and a UK level, data retention powers are not compatible with the ECHR irrespective of any mechanisms of access to, retention of, and notification of (retention or access) communications data. It further discusses with a focus on UK law that the judicial element of authorisation under the IPA 2016 would also unlikely to be compatible with the ECHR for lack of independence guaranteed – meaning that even if the

---

[397] ibid, [105].
[398] ibid, [75-77].
[399] ibid, [77].
[400] Christina Lienen, (n226).
[401] *Tele2 Sverige AB and Watson*, (n213), [121].
[402] Franziska Boehm and Paul de Hert, (n389); Franziska Boehm and Paul de Hert (n392).

JC and IPC had the power to issue ECHR compliant retention notices, the UK could still be in violation.

8. Conclusion:

EU law now appears to place a mandatory (or essential) requirement on Member States to put in place judicial or independent controls of access to communications data. In light of Brexit, and in order satisfy the 'adequacy' requirement, the UK may need to comply with such a requirement in any event, and it may be in the process of doing so.[403] However, what EU law has failed to acknowledge, is that such a requirement should not only apply to access to communications data, but the retention of said data. It has been argued, and acknowledged by the AG and the CJEU in *Tele2 and Watson*, that retention of communications data poses just as serious of an interference with privacy, freedom of expression and data protection as interception. Therefore, it would be sensible if the safeguards on retention of communications data met the requirements established in *Tele2 and Watson*. The UK has taken a step further than the EU in now requiring data retention notices to be approved by the JC and IPC. However, notwithstanding concerns of the JC and IPC's effectiveness, the jurisprudence of the ECtHR has already demonstrated that judicial control does not *ipso facto* constitute Convention compliance, notably in *Zakhakrov*, *Kruslin*, *Matheron*, and even before then with Lord Salmon's dissent in *Rossminster Ltd*. It is also true however, that judicial authorisation exists to ensure the greatest degree of independence and impartiality, which is only one of the many requirements of Article 8. The requirement of judicial authorisation is slowly creeping into provisions of interception, access to, and retention of, communications data. However, judicial authorisation of retention notices as they currently are would make no distinction between whose data is retained, as it is based on the service used and therefore the relationship between the interference and the aim pursued is not met.

This issue also persists at an EU level, although the CJEU ruled that general and indiscriminate data retention obligations on all services for all data of users and subscribers are no longer under EU law. This assumes in this particular context, the level of protection of the CFR is equal to the ECHR. However, the AG in *Tele2 and Watson* noted that the CFR should never be interior to the ECHR whilst simultaneously issuing an Opinion that produces an outcome of inferior protection. That is because even taking into account the CJEU's ruling, retention obligations would still be incompatible with the ECHR *irrespective* of the access mechanisms and even the mode of retention as envisaged by the CJEU, because again the interference (in many cases) would not correspond with any prior suspicion. In highlighting that there has been an oversight in protection, half-correcting that oversight would merely be another oversight in the proper protection of rights; and thus the only way to remedy this oversight is to ensure that retention notices (or more correctly defined as 'data preservation'[404]) or obligations '*must be used for a specific purpose, not as a general "fishing" exercise to bring in information*'[405] based on verifiable reasonable suspicion that is necessary and proportionate, through the least restrictive measure with a suitable notification system. Therefore, both at an EU and UK level, fundamental rights are not being fully respected, and thus constitute an oversight in protection.

---

[403] Home Office, (n28).
[404] Caspar Bowden, 'Digital Surveillance, Chapter Five Part I' (28 April 2013) <https://www.openrightsgroup.org/ourwork/reports/digital-surveillance/chapter-five-part-i> accessed 2 January 2017.
[405] *Kopp*, (n386).