Legal Studies (2021), **41**, 130–155
doi:10.1017/lst.2020.35

S·L·S
The Society of Legal Scholars

RESEARCH ARTICLE

Is the incompatibility of UK data retention law with EU law really a victory?

Matthew White*

Sheffield Hallam University, Sheffield, UK
* Author email: the_m_white@outlook.com

(Accepted 26 September 2020)

Abstract

The Court of Justice of the European Union (ECJ) in 2014 ruled in *Digital Rights Ireland* that the Data Retention Directive was invalid for exceeding the limits of proportionality in light of Articles 7, 8 and 52(1) of the EU Charter of Fundamental Rights (Charter). Subsequently, preliminary references from the England and Wales Court of Appeal and the Swedish Administrative Court of Appeal sought clarification from the ECJ as to whether EU law permitted 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. The ECJ in *Tele2 and Watson* ruled that in light of Articles 7, 8, 11 and 52(1) of the Charter, EU Member States were precluded from adopting national measures which provided general and indiscriminate retention of traffic and location data of all subscribers and registered users relating to all means of electronic communication. The ECJ also ruled that Member States were only permitted to adopt data retention measures for the purpose of fighting serious crime, and only when access to retained data was subject to prior review by a court or an independent administrative body.

In 2018, the issue of the UK's data retention regime envisaged in Part 4 of the Investigatory Powers Act 2016 came before the England and Wales High Court. The High Court ruled that Part 4 was incompatible with EU law because access to retained communications data was not limited to the purpose of fighting serious crime, and it was not subject to prior review by a court or an independent administrative body. This judgment was regarded by the claimants, Liberty, as a 'landmark victory for privacy rights'. However, this paper questions whether certain aspects of the High Court ruling are indeed a victory, by assessing its compatibility with EU law and the European Convention on Human Rights (ECHR).

Keywords: data retention; European Convention on Human Rights; Charter of Fundamental Rights; communications data; privacy; freedom of expression; religion; thought and consciousness; assembly and association

Introduction

In 2014, the Court of Justice of the European Union (ECJ) ruled in *Digital Rights Ireland*[1] that the Data Retention Directive[2] was invalid for exceeding the limits of proportionality in light of Articles 7 (private and family life, home and communications), 8 (protection of personal data) and 52(1) (scope of rights) of the EU Charter of Fundamental Rights (Charter).[3] Subsequently, preliminary references from the England and Wales Court of Appeal (Court of Appeal) and the Swedish

[1]Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Seitlinger and Others* [2014] 3 WLR 1607, Opinion of Cruz Villalón, para 73.

[2]Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L 105/54.

[3]Charter of Fundamental Rights of the European Union, OJ 2000 C364/01 and OJ 2010 C83/389.

Administrative Court of Appeal (Administrative Court)[4] sought clarification from the ECJ. The Administrative Court asked whether EU law permitted 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.[5] The ECJ in *Tele2 and Watson* ruled that in light of Articles 7, 8, 11 (freedom of expression) and 52(1) of the Charter, EU Member States were precluded from adopting national measures which provided general and indiscriminate retention of traffic and location data *of all subscribers and registered users relating to all means of electronic communication* (emphasis added).[6] Amongst other things, the ECJ also ruled that Member States were only permitted to adopt data retention measures for the purpose of fighting serious crime, and only when access to retained data was subject to prior review by a court or an independent administrative body.[7]

In 2018, the issue of the UK's data retention regime, as envisaged in Part 4 of the Investigatory Powers Act 2016 (IPA 2016), came before the England and Wales High Court (High Court).[8] The High Court ruled that Part 4 was incompatible with EU law because *access* to retained communications data was not limited to the purpose of fighting serious crime, and it was not subject to prior review by a court or an independent administrative body.[9] This judgment was regarded by the claimants, Liberty, as a 'landmark victory for privacy rights'.[10] However, this paper (which is based on and expands upon a blog post[11]) questions whether certain aspects of the High Court ruling are indeed a victory, by assessing the ruling's compatibility with EU law and the European Convention on Human Rights (ECHR).

1. Data retention under the Investigatory Powers Act and its incompatibility with EU law

(a) Data retention under the Investigatory Powers Act

The IPA 2016 was introduced to update the UK's framework for use of investigatory powers to obtain communications and communications data.[12] This new framework was lauded as establishing a 'world-leading oversight regime',[13] which introduced the Investigatory Powers Commissioner (IPC) and Judicial Commissioners (JCs) via section 227(1)(a) and (b) of the IPA 2016. The 2016 Act is the successor to much of the Regulation of Investigatory Powers Act 2000 and the Data Retention and Investigatory Powers Act 2014 (DRIPA 2014). The latter was declared to be incompatible with EU law by the Court of Appeal for the same reasons as the IPA 2016.[14]

The data retention regime in the IPA 2016 is set out in Part 4. Section 87(1) permitted the Secretary of State, if it is considered necessary and proportionate, to issue retention notices on telecommunications operators to retain relevant communications data for purposes (a) to (j) in section 61(7). These grounds, amongst others, were included in the interests of national security, for the purpose of

[4]Opinion of Saugmandsgaard Øe in Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB and Watson and Others* [2016] ECR I-572, para 5.

[5]Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB and Watson and Others* [2017] 2 WLR 1289, para 51.

[6]Ibid, para 134(1).

[7]Ibid, para 134(2).

[8]*Liberty v Secretary of State for the Home Department and Others* [2018] 3 WLR 1435.

[9]Ibid, para 186.

[10]Liberty 'Liberty wins first battle in landmark challenge to mass surveillance powers in the Investigatory Powers Act' 27 April 2018, https://www.libertyhumanrights.org.uk/issue/liberty-wins-first-battle-in-landmark-challenge-to-mass-surveillance-powers-in-the-investigatory-powers-act/ (accessed 4 November 2020).

[11]M White 'Data retention incompatible with EU law: victory? Victory you say?' 24 May 2018, https://eulawanalysis.blogspot.com/2018/05/data-retention-incompatible-with-eu-law.html (accessed 4 November 2020).

[12]Explanatory Notes to the Investigatory Powers Act 2016, para 1.

[13]T 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 4 November 2020).

[14]*Tom Watson and Others v Secretary of State for the Home Department* [2018] 2 WLR 1735, paras 27–29.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

preventing or detecting crime or of preventing disorder, in the interests of public safety, etc. A retention notice is only permissible once it has been approved by a JC.[15]

Relevant communications are defined in section 87(11) as any communications data which may be used to identify, or assist in identifying:

(a) the sender or recipient of a communication (whether or not a person);
(b) the time or duration of a communication;
(c) the type, method or pattern, or fact, of communication;
(d) the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted; or
(e) the location of any such system; this expression therefore includes, in particular, internet connection records.

This definition covers any type of communication network including communications where the sender and receiver are not humans, such as background interactions on smartphones, but probably also the Internet of Things.[16] Section 261(5) of the IPA 2016 defines communications data as either being events data or entity data. For the purposes of this paper, only the latter will be considered in detail. Events data is defined in section 261(4) as:

> any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time.

The Explanatory Notes to the Act maintain that events data includes:

> [t]he fact that someone has sent or received an email, phone call, text or social media message; the location of a person when they made a mobile phone call or the Wi-Fi hotspot that their phone connected to; or the *destination IP address* that an individual has connected to online.[17]

The Communications Data Code of Practice (Code of Practice) lists several examples of what constitutes events data:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and email headers – to the extent that content of a communication, such as the subject line of an email, is not disclosed);
- itemised telephone call records (numbers called)
- itemised internet connection records;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;

[15]IPA 2016, s 87(1)(b).

[16]G Smith 'Never mind internet connection records, what about relevant communications data?', *Cyberleagal* 29 November 2015, https://www.cyberleagle.com/2015/11/never-mind-internet-connection-records.html (accessed 4 November 2020).

[17]Explanatory Notes to the Investigatory Powers Act 2016, para 727.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to), including conference calling, call messaging, call waiting and call barring telecommunications services.[18]

Entity data is defined in section 261(3) as any data which:

(a) is about—
  (i) an entity,
  (ii) an association between a telecommunications service and an entity, or
  (iii) an association between any part of a telecommunication system and an entity,
(b) consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity's location), and
(c) is not events data.

'Entity' is defined as a person or thing.[19] This could be individuals, groups or objects,[20] such as 'phones, tablets and computers'.[21] Entity data includes phone numbers or other identifiers linked to communication devices, such as IP addresses (allocated by an internet access provider).[22] The Code of Practice explains further that entity data can include devices:

> so this data would cover information about the devices owned by a customer as well as the services provided by the telecommunications operator to which the owner of the devices subscribes… [and]… names and addresses of subscribers.[23]

Additionally it includes:

- 'subscriber checks', such as 'who is the subscriber of phone number 01234 567 890?', 'who is the account holder of email account example@example.co.uk?' or 'who is entitled to post to web space www.example.co.uk?';
- subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes; and
- information about selection of preferential numbers or discount calls.

This would include, as Liberty notes, 'information about all applications ("apps") mobile phone or internet service subscribers have installed on their phone or as an add-on to their primary service'.[24]

[18]Home Office 'Communications Data Code of Practice' November 2018, para 2.45, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf (accessed 4 November 2020).

[19]IPA 2016, s 261(7).

[20]Explanatory Notes to the Investigatory Powers Act 2016, para 725.

[21]Communications Data Code of Practice, above n 18, para 2.38.

[22]Explanatory Notes to the Investigatory Powers Act 2016, para 727.

[23]Communications Data Code of Practice, above n 18, para 2.24.

[24]Liberty, 'Liberty's response to the Government's consultation on the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data (proposed amendments to the Investigatory Powers Act 2016 and Communications Data Code of Practice)' 18 January 2018, para 55 https://web.archive.org/web/20180626165837/https://www.libertyhumanrights.org.uk/sites/default/files/2018.01.18%20liberty%20consultation%20response%20FINAL.pdf (accessed 5 November 2020)

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

This can include which bank a person uses, where investments reside, what newspapers are read, whether a person has children, their sexuality and even whether one is having or contemplating having an affair.[25]

(b) The Investigatory Powers Act before the High Court

Following the ECJ's ruling in *Tele2 and Watson*, judicial review proceedings challenging the legality the IPA 2016 were initiated on 28 February 2017.[26] The High Court acknowledged that the proceedings concerned the Charter and the ECHR[27] but went on to only consider the Charter.[28] The High Court noted that the defendants conceded that the IPA 2016 was incompatible with EU law in two respects.[29] However, these inconsistencies were unamended, and thus the claimants argued that unlawful retention and access persisted.[30]

In the dispute about what was the appropriate remedy, the defendants argued that no more than declaratory relief was necessary,[31] because the concession on inconsistency had already been made.[32] The claimants argued for a suspended disapplication, which the High Court believed was fair.[33] However, the High Court decided not to issue a disapplication, or a declaration[34] and instead gave the UK Government until 1 November 2018 to amend the IPA 2016.[35]

The High Court also examined whether the IPA 2016 permitted general and indiscriminate data retention. The Court of Appeal's interpretation of the DRIPA 2014 was considered[36] and it was concluded that the IPA 2016 did not provide for general and indiscriminate data retention.[37]

Additionally, the High Court considered the question of whether entity data fell within the scope of traffic data or location data in *Tele2 and Watson*,[38] as defined in Articles 2(b) and (c) of the ePrivacy Directive as follows:[39]

> (b) 'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;
> (c) 'location data' means 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.

The claimants argued that ultimately this was and should be for the ECJ to decide, whereas the defendants argued that it was not and that this was *acte clair*.[40] The High Court agreed with the defendants that entity data did not fall within the definitions of traffic or location data,[41] thus putting it

[25]Ibid, para 56.
[26]*Liberty*, above n 8, para 5.
[27]Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950.
[28]*Liberty*, above n 8, para 2.
[29]Ibid, para 8.
[30]Ibid, para 9.
[31]Ibid, para 32.
[32]Ibid, paras 31 and 28.
[33]Ibid, para 42.
[34]Ibid, para 105.
[35]Ibid, para 187.
[36]*Tom Watson and Others v Secretary of State for the Home Department*, above n 14, paras 22–26.
[37]*Liberty*, above n 8, para 138.
[38]Ibid, para 139.
[39]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201/37.
[40]*Liberty*, above n 8, para 139.
[41]Ibid, para 151.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

outside the scope of EU law.[42] The High Court also felt satisfied that this issue was *acte clair*, and thus declined to issue a preliminary reference.[43]

Finally, the High Court considered the seriousness threshold for all retention objectives. The claimants argued that this seriousness threshold should be applied to the section 61(7) purposes for issuing a retention notice in the IPA 2016.[44] The High Court referred to this argument being rejected by the Court of Appeal and noted that this position remained undisturbed by the ECJ's judgment.[45] The High Court held that the fact that the IPA 2016 did not impose a seriousness threshold on a permissible objective for issuing a retention notice, does not render it incompatible with EU law.[46] The High Court continued that such considerations of seriousness do not apply to other objectives, such as national security, public safety and miscarriages of justice.[47] The High Court felt that the tests of necessity and proportionality found within section 87(1) adequately dealt with the issue of seriousness.[48] The High Court also pointed to the claimant's counsel, Mr Jaffey, who acknowledged that 'a threat to national security would readily cross' the threshold for seriousness.[49]

Ultimately, the High Court ruled that Part 4 was incompatible with EU law for lack of prior authorisation by a court or an independent administrative body for access to communications data[50] because the JC approvals had not yet come into force.[51] It was also held to be incompatible with EU law because *access* to *retained data* was not limited to fighting serious crime.[52]

2. Is the High Court's ruling a victory?

(a) Ignoring the European Convention on Human Rights

It is unfortunate that the High Court decided not to consider the ECHR in combination with the Charter, as the interpretation of the Convention in relation to measures of secret surveillance and data retention is of the utmost relevance. It is also unfortunate because where the Charter contains rights which correspond to those in the ECHR, the meaning and scope of those rights shall be interpreted in the same way,[53] and this could have been a useful guide for the High Court. This failure to consider the ECHR, and the impact of that failure on the flawed reasoning of the High Court, will be highlighted throughout the following text.

(b) Data retention does not concern the content of communications?

The High Court stressed that Part 4 of the IPA 2016 does not concern the *content* of communications such as emails or text messages.[54] Emails and text messages are but two examples of content. Content is defined in section 261(6) of the IPA 2016 as any element of the communication, or data logically associated with it, which reveals anything of what might reasonably considered as the *meaning* of the communication. This excludes inferences that can be drawn from communications[55] and systems data. 'Systems data' is defined in section 263(4) as data which may be used:

[42]Ibid, paras 151 and 154.
[43]Ibid, para 155.
[44]Ibid, para 156.
[45]Ibid, paras 157–158.
[46]Ibid, para 158.
[47]Ibid, para 161.
[48]Ibid,
[49]Ibid.
[50]Ibid, para 186.
[51]Ibid, para 132.
[52]Ibid,
[53]Art 52(3) of the Charter.
[54]*Liberty*, above n 8, para 3.
[55]Explanatory Notes to the Investigatory Powers Act 2016, para 728.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

a. to identify, or assist in identifying, any person, apparatus, system or service;
b. to identify any event; or
c. to identify the location of any person, event or thing.[56]

The distinction between content and communications data has been used by courts in the UK to suggest that content is more intrusive than communications data.[57] However, it has been argued that communications data is just as revealing as content,[58] if not more so.[59] For this reason, the UN Office of the High Commissioner for Human Rights (OHCHR) has decided that the distinction between content and communications data is no longer tenable.[60] Moreover, the European Court of Human Rights (ECtHR) has stressed that the principles with regard to interception are not based on the *technical* definition of interference, but on the *level* of interference,[61] and thus it is argued that the same principles should apply in the communications data context. Moreover, the ECtHR is 'not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content'.[62] This demonstrates that the UK can no longer rely on the purported distinction between communications data and content to justify differential treatment.

Schneier argues that communications data gives us context,[63] and context gives us meaning.[64] The effect of communications data is that 'a very comprehensive dossier on an individual's private life can be produced (including contacts, where he or she has been, is, or will be going, and his or her interests and habits)'.[65] Some argue that although content may not be revealed, content-related conclusions can be drawn[66] on what kind of content is being viewed.[67] This demonstrates the problematic construction of the IPA 2016, section 261(6), in that it proclaims that context is meaning, but not the kind of meaning that can be gained from communications data, thus illustrating that 'meaning' is unclear, because what if the same meaning of a communication could be obtained from communications data? Additionally, Cobbe points out that Parliament has not chosen to carry over a definition from DRIPA 2014 to the IPA 2016 that generally excluded content from communications data,[68] thus implying that content *can* be retained. Furthermore, Cobbe notes that the 'meaning' of a communication is unclear, and neither is it 'clear that data revealing the meaning of a communication is the same as data providing knowledge of its content',[69] as the ECJ suggest (see below).

[56]Explanatory Notes to the Investigatory Powers Act 2016, para 735.

[57]*R (on the application of Davis & Others) v Secretary of State for the Home Department & Others* [2015] WLR(D) 318, para 81; *Liberty and Others v Government Communication Head Quarters and Others* [2015] 3 All ER 142, paras 34, 111 and 114.

[58]E Fura and M Klamberg 'The chilling effect of counter-terrorism measures: a comparative analysis of electronic surveillance laws in Europe and the USA' in J Casadevall et al (eds) *Freedom of Expression – Essays in Honour of Nicolas Bratza – President of the European Court of Human Rights* (Oisterwijk: Wolf Legal Publishers, 2012) p 467; Opinion of Saugmandsgaard Øe in *Tele2 Sverige AB and Watson*, above n 4, para 254.

[59]A Escudero-Pascual and I Hosein 'Questioning lawful access to traffic data' (2004) 47 Communications of the ACM 82; Opinion of Saugmandsgaard Øe in *Tele2 Sverige AB and Watson*, above n 4, para 259.

[60]Report of the Office of the High Commissioner for Human Rights 'The right to privacy in the digital age' 2014, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (accessed 4 November 2020) para 19.

[61]*RE v UK* (2016) 63 EHRR 2, para 130.

[62]*Big Brother Watch and Others v UK* [2018] ECHR 58170/13, para 356.

[63]B Schneier *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (WW Norton, 2016) p 26.

[64]P Tompkins and J Lawley 'Context matters' 5 April 2003, http://www.cleanlanguage.co.uk/articles/articles/205/1/Context-Matters/Page1.html (accessed 4 November 2020).

[65]N Taylor 'Policing, privacy and proportionality' (2003) 86 EHRLR 97.

[66]Bundesverfassungsgericht 'Data retention unconstitutional in its present form' March 2010 https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html (accessed 4 November 2020).

[67]J Saiban and J Sykes 'UK Anti-Terrorism Act 2001 and ISPs: a cyber check-point Charlie?' (2002) 18 Computer Law & Security Review 338; D Solove 'Reconstructing electronic surveillance law' (2004) 72 George Washington Law Review 1264.

[68]J Cobbe 'Casting the dragnet: communications data retention under the Investigatory Powers Act' (2018) PL 14.

[69]Ibid, at 14.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

Not only can communications data be just as revealing as content, if not more so; content within communications data can *itself* still be revealed. iiNet demonstrated that embedded data about communications like Twitter, Facebook, and websites do in fact reveal the content of communications (such as tweets), and a great deal of it.[70]

Furthermore, the High Court narrowly considered section 87(1) of the IPA 2016 in isolation, and thus, for example, did not contemplate section 87(4)(d) of the Act. That provision stipulates that retention notices must not require telecommunications operators to retain data that is not used by them for a lawful purpose. Lawful purposes are not defined in the IPA 2016, but section 46(4)(a) allows (by regulation, section 46(1) and (2)) any business to conduct interception if it constitutes a legitimate practice reasonably required for the purpose, in connection with the carrying on of any relevant activities for the purpose of record keeping. Section 46(2)(b) includes communications relating to business activities, essentially permitting interception for 'business purposes'. This business purpose rationale would be consistent with the Home Office's approach to deep packet inspection as they considered that it was 'a term used to describe the technical process whereby many communications service providers currently identify and obtain communications data from their networks for their *business purposes*'.[71] The European Data Protection Supervisor has stated that deep packet inspection enables internet service providers (ISPs) to access information addressed to the recipient of the communication only, which requires the interception of communications data *and content*.[72] This could permit intercepted data to be retained,[73] which in turn could constitute a lawful purpose under section 87(4)(d).

Neither did the High Court consider internet connection records, which fall under the umbrella of relevant communications data. 'Internet connection records' is defined in the IPA 2016, section 62(7)(a) and (b) as communications data which:

(a) may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and
(b) comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).

The explanatory notes to the Act explain that internet connection records include websites.[74] Obtaining website names[75] and internet connection records would require deep packet inspection,[76] and thus content *would* be obtained. These are but a few examples (data can also be generated via section 87(9)(b), and could include the content of communications) which demonstrate that the

[70]iiNet 'Protecting your privacy: our stand against "mandatory data retention"' 21 July 2014, http://blog.iinet.net.au/protecting-your-privacy/ (accessed 4 November 2020).

[71]Home Office 'Protecting the public in a changing communications environment' November 2009, para 15, http://webarchive.nationalarchives.gov.uk/+/http:/www.homeoffice.gov.uk/documents/cons-2009-communication-data/cons-2009-comms-data-responses2835.pdf?view=Binary (accessed 4 November 2020).

[72]Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data 2012/C 34/01, para 32.

[73]Joint Committee on the Draft Investigatory Powers Bill "Written evidence" February 2016, Open Rights Group, para 125, p 1104 http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf (accessed 4 November 2020).

[74]Explanatory Notes to the Investigatory Powers Act 2016, para 265.

[75]S Stalla-Bourdillon 'What the hell are these metadata? … Are communications data, traffic data and metadata all the same thing?' 30 October 2014, https://peepbeep.wordpress.com/2014/10/30/what-the-hell-are-these-metadata-are-communications-data-traffic-data-and-metadata-all-the-same-thing/ (accessed 4 November 2020); S Stalla-Bourdillon et al 'Metadata, traffic data, communications data, service use information… What is the difference? Does the difference matter? An interdisciplinary view from the UK' in S Gutwirth et al (eds) *Data Protection on the Move* (Springer, 2016) p 441.

[76]Written evidence submitted by Exa Networks Ltd (IPB0026) paras 23–25; Written evidence submitted by IT-Political Association of Denmark (IPB0051) para 21; Written evidence submitted by Open Rights Group (IPB0034) para 6.2.3.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

High Court's narrow focus on section 87(1) blinded it to the fact that communications data is just as revealing as content, if not more so, and – in any event – content would be retained too.[77] This would permit knowledge of the content to be acquired, which would adversely affect or compromise the essence of the protected rights,[78] contrary to EU law.

(c) Entity data does not fall within the scope of EU law?

The High Court rejected the argument that entity data (such as addresses, specific locations, billing address and details) fell within the definition of traffic and location data.[79] The High Court referred to the idea that traffic data is concerned with the conveyance of a communication, and thus only concerns itself with data for the billing of such a communication, and not billing data in general.[80] For the High Court, the mere holding of a billing address or bank details does not fall within the billing limb of traffic data,[81] and itemised billing would fall within the definition of traffic data, and in any case would be events data.[82]

This construction is problematic for a variety of reasons. Even if one were to assume the High Court was correct, this would ignore the ePrivacy Directive and EU data protection laws. As discussed above, events data does *not* include information on addresses, billing and payment methods etc; this would be entity data, as it identifies an individual. Although the High Court did rely on Recital 27 of the ePrivacy Directive to justify its reasoning, it misunderstood it, and overlooked other articles and recitals. The High Court justified its reliance on Recital 27 by asserting that because traffic data should be erased (except for billing purposes), this places the holding of billing addresses or bank account details outside the 'billing' limb of traffic data. The High Court also referred to Article 6 to support this position. However, although Article 6(1) states that traffic data must be erased when it is no longer needed for the transmission of a communication, this is without prejudice to Article 6(2), (3), (5) and Article 15(1). When Article 6(2) is examined, it clearly states that:

> [t]raffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

Not only does Article 6(2) essentially assert that subscriber data is traffic data, which would make it entity data, it also states that this data can be held only for as long as the bill can lawfully be challenged or payment be pursued. This indicates that traffic data beyond the purposes necessary for the transmission of a communication would equate to entity data, as billing addresses and details would come within the ambit of Article 6(2) because they would be necessary for billing and interconnection payments. The High Court seemingly misunderstood Recital 27, by considering it in isolation from Recital 29, for example. Recital 29 states that traffic data necessary for billing purposes may be processed to prevent fraud.

Similarly, the High Court failed to consider Recital 26 of the ePrivacy Directive, which implicitly expands upon Article 6(2), stating that:

> The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate

[77] White, above n 11.

[78] *Digital Rights Ireland Ltd v Seitlinger and Others* [2014] All ER (EC) 775, para 39; Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* [2016] QB 527, [2016] 2 WLR 873, para 94.

[79] *Liberty*, above n 8, para 151.

[80] Ibid, para 152.

[81] Ibid.

[82] Ibid.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

> interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time.

Liberty highlighted that Article 1 (Scope and aim) and 3 (Services concerned) of the ePrivacy Directive concern the processing of personal data in the electronic communications sector.[83] As the Code of Practice (see above) states, subscriber information falls within the ambit of entity data, and thus falls within the ambit of the ePrivacy Directive. Article 15(1) stipulates that 'Member States may, inter alia, adopt legislative measures providing for the retention of data'. This does not specifically refer to traffic or location data, even if one were to argue that entity data does not fit with either definition. Moreover, when one considers the now invalid Data Retention Directive,[84] Article 1(2) of that Directive provided that it applied to 'traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user'. This is an important point, because the UK's ability to adopt data retention measures arises from Article 15 (1).[85] The ePrivacy Directive and the invalid Data Retention Directive both support the notion that entity data is within the scope of EU law.

Additionally, the High Court's reasoning relied upon the definition of traffic data in isolation from the definition of 'communication' in the ePrivacy Directive.[86] Communication includes 'any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service'. Recital 15 of the ePrivacy Directive states that a communication:

> may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission.

The Article 29 Data Protection Working Party regarded traffic data as including, amongst other things, the email and IP address of the sender, email address of the receiver and the date and time of the email being sent.[87] As the Code of Practice (see above) states, IP addresses and subscriber information (such as email addresses) fall within the ambit of entity data.

Recital 46 of the ePrivacy Directive states that 'Directive 95/46/EC covers any form of processing of personal data regardless of the technology used'. The ECJ has ruled that the term personal data is wide in scope, not restricted to sensitive or private information, and potentially encompasses all kinds of information, whether it be objective or subjective, provided that it relates to the data subject.[88] This can include anything from a name, photo, email address, bank details, GPS tracking data, posts on social networking websites, medical information or a computer's IP address.[89] Thus, even if the definitions in the ePrivacy Directive did not apply, processing (which includes collecting, recording and storing,[90] ie retention) entity data would still be subject to the General Data Protection

[83]Liberty, above n 24, paras 43–44.

[84]Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC OJ L 105.

[85]*Tele2 Sverige AB and Watson and others*, above n 5, para 74.

[86]Art 2(d).

[87]Art 29 Data Protection Working Party 'Privacy on the internet – an integrated EU approach to on-line data protection' 21 November 2000, para 33, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf (accessed 4 November 2020).

[88]Case C-434/16, *Peter Nowak v Data Protection Commissioner* [2018] 1 WLR 3505, para 34.

[89]European Union Agency for Fundamental Rights 'Handbook on European data protection law' 2018, para 350, http://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (accessed 4 November 2020).

[90]Art 4(2) of the General Data Protection Regulation.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

Regulation,[91] (because, for example, IP addresses are entity data, and can constitute personal data) and thus within the scope of EU law, and ultimately, within the scope of the Charter – particularly Article 8, which eclipses the General Data Protection Regulation.[92]

The ECJ's position in *Tele2 and Watson* confirms the scope of the ePrivacy Directive as regulating activities of providers of electronic communications services.[93] It also confirms that the Directive applies to the measures taken by all persons other than users – whether that be private persons, bodies or the State – in the prevention of unauthorised access to communications *including any data* related to such communications.[94] The ECJ concluded that issues raised by the Court of Appeal and Administrative Court fell within the scope of the ePrivacy Directive.[95] Additionally, the ECJ did not limit its interpretation of data retention within the confines of the ePrivacy Directive (to publicly available electronic communications services); instead its interpretation included 'all means of electronic communication, and that it imposes on providers of electronic communications services an obligation to retain that data systematically and continuously, with no exceptions'.[96] The ECJ continued that communications data included data 'relating to subscriptions and all electronic communications necessary to trace and identify the source and destination of a communication'.[97] Furthermore, the ECJ held that communications data included the 'name and address of the subscriber or registered user, the telephone number of the caller, the number called and an IP address for internet services'.[98] These sets of communications data would *all* fall under the ambit of entity data.

Big Brother Watch also observed this point, explaining that '[the ECJ's] judgment did not distinguish different standards for traffic and location data to those for other communications data, but rather considered the national communications data regime as a whole'.[99] Big Brother Watch also noted that in the Court of Appeal's 2015 judgment on the DRIPA 2014,[100] the Court expressly referred to the communications data retention regime as a whole, identifying *all* the communications data contained.[101] Furthermore, the ECJ, as mentioned above, ruled that general and indiscriminate 'retention of traffic and location data of all subscribers and registered users relating to all means of electronic communication' is precluded by EU law. This, again, would put entity data within the scope of EU law.

The ECJ took this approach (consistent with the ECtHR's lack of interest in technical definitions) because the ePrivacy Directive was read in the light of the Charter.[102] Thus, when the High Court ruled that entity data fell outside the scope of EU law, it did so by ignoring the ePrivacy Directive, EU data protection law and the ECJ's interpretation in *Tele2 and Watson*. Thus, in reality, it was *acte clair* that entity data was *within* the scope of EU law. As Big Brother Watch note, '[e]ven on the basis of the Government's restrictive and incorrect interpretation of the [ECJ's] judgment, the judgment still applies to both "events" and "entity" data'.[103] This is problematic not only because the High Court erred in its interpretation of EU law; it also means that if entity data is not subject

[91]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

[92]A Murray 'Data transfers between the EU and UK post Brexit?' (2017) 7(3) International Data Privacy Law 151.

[93]*Tele2 Sverige AB and Watson and Others*, above n 5, para 70.

[94]Ibid, para 77.

[95]Ibid, para 81.

[96]Ibid, para 97.

[97]Ibid, para 17.

[98]Ibid, para 98.

[99]Big Brother Watch 'Big Brother Watch's response to the Government's consultation on the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention and acquisition of communications data' January 2018, para 4, https://bigbrotherwatch.org.uk/wp-content/uploads/2018/01/Big-Brother-Watch-Response-to-the-Watson-Consultation-Jan-2018.pdf (accessed 4 November 2020).

[100]*Secretary of State for the Home Department v Davis MP & Others* [2015] EWCA Civ 1185, para 5.

[101]Big Brother Watch, above n 99, para 4.

[102]*Tele2 Sverige AB and Watson and Others*, above n 5, para 134(1) and (2).

[103]Big Brother Watch, above n 99, para 5.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

to EU law, the safeguards that come with the General Data Protection Regulation and the interpretations of *Digital Rights Ireland* and *Tele2 and Watson* are not applicable, creating a disparity in fundamental rights protection. If the High Court were a court of last instance, this could engage state liability for committing a manifest breach of EU law.[104]

Moreover, due to High Court's failure to consider the ECHR, the Court failed to outline the limits of retaining entity data which would be compatible with the ECHR. The relevance of compatibility with the ECHR becomes crucial (see below); Big Brother Watch even remark that the definition of entity data in the IPA 2016 (see above), notably where data that identifies or describes an entity, whether or not by reference to the entity's location 'explicitly includes location data'.[105] The High Court ruled that entity data does not fall within the ambit of location data because, for example, the location of a fixed-line terminal is simply held by a service provider and is not processed in a communications network or by communications service.[106] However, the High Court was not clear on what is meant by a service provider. The ePrivacy Directive throughout equates public communications network or publicly available electronic communications service as service providers. If the High Court meant that a service provider can be either a communications network or service, then its understanding of data protection laws is unsound. As discussed above, the mere storage of personal data constitutes a form of processing. Thus, service providers who hold or store the location of a fixed-line terminal are processing that data. The distinction between processing and holding data displays a fundamental misunderstanding of what actually constitutes processing. To further highlight the High Court's error, the Code of Practice states that links between a person and their phone are entity data.[107] The Code of Practice describes IP addresses of an individual as entity data, and states that this is important because 'your IP address is the address or logical location of your computer when it's connected to the Internet'.[108] Article 2(c) of the ePrivacy Directive specifies that location data is any data processed that indicates the geographical position of the terminal equipment, ie the location of one's computer. Recital 15 states that traffic data 'consist[s] of data referring to the… location of the terminal equipment of the sender'. The Article 29 Working Party highlighted that geolocation of IP addresses is one of the many ways of processing location data.[109] Entity data also consists of identifiers linked to communication devices, such as a MAC address. These are unique hardware numbers for computers.[110] Edward Snowden has argued that the NSA has a system that tracks the movements (and therefore location) of everyone in a city by monitoring their MAC addresses,[111] Cunche accepts that this is a real possibility,[112] given that traffic and retail store monitoring are already occurring.[113] Banks maintains that 'there is a greater probability of correlation between the owner of the device and the MAC address than there is of an IP address and an individual'.[114] This is conceivable because IP

[104]X Groussot and T Minssen 'Res judicata in the ECJ case law: balancing legal certainty with legality?' (2007) 3 EuConst 385.

[105]Big Brother Watch, above n 99, para 5.

[106]*Liberty*, above n 8, para 153.

[107]Communications Data Code of Practice, above n 18, para 2.38.

[108]WhatIsMyIPAddress 'What's behind your IP address?' https://whatismyipaddress.com/ip-reveal (accessed 4 November 2020).

[109]Article 29 Data Protection Working Party 'Opinion 13/2011 on geolocation services on smart mobile devices' 16 May 2011, para 3, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf (accessed 4 November 2020).

[110]M Rouse 'MAC address (media access control address)' 19 April 2017 http://searchnetworking.techtarget.com/definition/MAC-address (accessed 4 November 2020). For a more technical definition see M Cunche 'I know your MAC address: targeted tracking of individual using wi-fi' (2014) 10(4) Journal of Computer Virology and Hacking Techniques https://hal.inria.fr/hal-00858324/document (accessed 4 November 2020).

[111]J Bamford 'The most wanted man in the world' 13 June 2014 http://www.wired.com/2014/08/edward-snowden/ (accessed 4 November 2020).

[112]Cunche, above n 110.

[113]Ibid.

[114]T Banks 'MAC and IP addresses: personal information?' 24 July 2012 https://www.lexology.com/library/detail.aspx?g=1a45fb24-42dd-4608-b41b-9ed6d54a75ab (accessed 5 November 2020).

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

addresses can be dynamic – ie the IP address changes each time there is a new connection to the internet – as highlighted in *Breyer*,[115] whereas MAC addresses are not (unless hidden by the device owner).[116] What this demonstrates is that not only does entity data fall within the ambit of traffic data, it also falls within the ambit of location data, and is, in any event, within the scope of EU law.

Lastly, as noted above, the High Court ruled that the IPA 2016 was incompatible with EU law because access to retained data is not limited to the purpose of fighting serious crime. This passage confused their position on entity data because entity data is also retained. The High Court effectively placed entity data outside the scope of EU law whilst simultaneously ruling that data retained is within the scope of EU law, hence the requirement of combatting serious crime. A ruling that 'access to retained events data is limited to the purpose of combating "serious crime"' would have properly reflected the Court's reasoning. Simply put, its ruling does not reflect its own analysis.

(d) Seriousness threshold

When ruling that it was unnecessary to have a seriousness threshold for the purposes of retention, the High Court did not consider that the retention of communications data poses just as serious (if not more serious) an interference with fundamental rights as interception does. Section 20(2)(b) of the IPA 2016 in relation to interception warrants does have a seriousness threshold. Moreover, the UK Government has sought to comply with *Digital Rights Ireland/Tele2 and Watson* by inserting into the 2016 Act a definition of serious crime for the purposes of Part 4.[117] This new definition, however, has been argued to broaden the definition that is already present in the IPA 2016,[118] which is also beyond what the ECtHR accepted in *Kennedy*[119] and has been severely condemned by Liberty for creating a conflicting, confusing and overbroad standard for when communications data can be retained.[120] Ultimately, it does not provide 'adequate protection against abuse and is a serious problem regarding the protection of human rights'.[121]This highlights that a well-defined seriousness threshold *is* necessary.

The High Court also ruled that miscarriages of justice were a legitimate purpose for requiring data retention. However, from the perspective of the ECtHR, for measures to be 'in accordance with the law, they must be foreseeable, meaning the law must be formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate their conduct'.[122] This ensures that there is adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any such measures,[123] thus allowing individuals to avoid exposure to unwelcome intrusions by the state.[124] 'Miscarriages of justice' is not defined or explained, and thus lacks foreseeability.

The High Court also said that threats to national security would readily cross the threshold of seriousness. However, national security cannot, in and of itself, be used as justification for data retention. Judge Pettiti in *Kopp* stated that numerous European states have failed to comply with Article 8 by

[115]Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2017] 1 WLR 1569, para 16.

[116]C Hoffman 'How (and why) to change your MAC address on Windows, Linux, and Mac' 30 June 2014 https://www.howtogeek.com/192173/how-and-why-to-change-your-mac-address-on-windows-linux-and-mac/ (accessed 4 November 2020).

[117]Data Retention and Acquisition Regulations 2018, SI 2018/1123, reg 21, which inserts s 86(2A) into the IPA 2016.

[118]N Brown 'The CLOUD Act: cross-border law enforcement and the internet' 8 April 2018, https://www.scl.org/articles/10183-the-cloud-act-cross-border-law-enforcement-and-the-internet (accessed 4 November 2020).

[119]*Kennedy v UK* (2011) 52 EHRR 4, para 159.

[120]Liberty, above n 24, paras 4–8.

[121]M White 'Data retention: serious crime or a serious problem?' (2019) Public Law 643.

[122]*Amann v Switzerland* (2000) 30 EHRR 843, para 56.

[123]*Uzun v Germany* (2011) 53 EHRR 24, para 61.

[124]Privacy International 'Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights' 10 October 2003, para 3, http://www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf (accessed 4 November 2020).

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

abusing concepts such as national security, by distorting its meaning and nature,[125] with abuse by the UK well documented.[126] The ECtHR has decided that in the area of national security, Member States only enjoy a certain margin of appreciation and that[127] the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to prevent arbitrary interferences.[128] The ECtHR ruled that it was 'significant' that Russian law did 'not give any indication of the circumstances under which an individual's communications may be intercepted on account of events or activities endangering Russia's national… security'.[129] The High Court's assumption that a threat to national security in and of itself justifies data retention is problematic, as the IPA 2016 does not define national security in any way, nor are the circumstances in which it is to be relied upon clear.[130] Thus, data retention on this ground is insufficiently clear for the purposes of the ECHR.

(e) Access only for serious crime, but what about retention?

When ruling that Part 4 of the IPA 2016 was incompatible with EU law because it did not limit access only to cases involving serious crime, the High Court yet again erred in its interpretation of *Tele2 and Watson*. The ECJ ruled that '*only* the objective of fighting serious is capable of justifying [data retention]',[131] and failure to comply would also violate Article 8 of the ECHR.[132] Thus, when the High Court ruled that miscarriages of justice were sufficient to justify data retention, it was done in contravention of EU law and the ECHR. Additionally, an often overlooked aspect of the earlier ECtHR ruling in *Klass and Others* was where it ruled that '[s]ecret surveillance and its implications are facts that the Court, *albeit to its regret*, has held to be necessary, in modern-day conditions in a democratic society, *in the interests of national security and for the prevention of disorder or crime*' (emphasis added).[133] This demonstrates that not all the exemptions under Article 8 can be used to justify secret surveillance such as data retention.

This also creates another problem. If miscarriages of justice, for example, are a sufficient justification for data retention, why would the High Court then rule that access has to be limited to fighting serious crime? On the one hand, what would be the purpose of retaining data on the ground of miscarriages of justice, if that same data could not be accessed on that ground? On the other hand, if data is retained on the ground of miscarriages of justice and accessed on that same ground, this would go against the High Court's own ruling in limiting access to fighting serious crime. If data is retained on the ground of fighting serious crime but then accessed on the ground on miscarriages of justice, this creates issues of processing data for an incompatible purpose. Ben Emmerson QC and Helen Mountfield have stated that there would be a significant risk of a violation of Article 8 of the

[125] *Kopp v Switzerland* (1999) 27 EHRR 91.

[126] M White 'The threat to the UK's independent and impartial surveillance oversight' (2019) 5 European Human Rights Law Review 524–525; L Harding 'The State of Secrecy by Richard Norton-Taylor review – spooks in the spotlight' 10 February 2020, https://www.theguardian.com/books/2020/feb/10/state-of-secrecy-spies-media-britain-richard-norton-taylor-review (accessed 4 November 2020); J Grierson et al 'Putting extinction rebellion on extremist list "completely wrong", says Keir Starmer' 13 January 2020, https://www.theguardian.com/environment/2020/jan/13/priti-patel-defends-inclusion-of-extinction-rebellion-on-terror-list (accessed 4 November 2020); V Dodd and J Grierson 'Terror police's Extinction Rebellion "risk report" sent out a year ago' 6 February 2020 https://amp.theguardian.com/environment/2020/feb/06/terrorism-police-assessed-extinction-rebellion-earlier-than-thought?CMP=share_btn_tw&__twitter_impression=true (accessed 4 November 2020).

[127] *Roman Zakharov v Russia* (2016) 63 EHRR 17, para 232.

[128] Ibid, para 247.

[129] Ibid, para 248.

[130] M White 'Coronaveillance: coronavirus, a threat to national security, economic well-being and serious crime? Exposing pre-existing and ex post facto deficiencies in the Investigatory Powers Act?' (forthcoming).

[131] *Tele2 Sverige AB and Watson and Others*, above n 5 para 102.

[132] *Big Brother Watch and Others*, above n 62, paras 465–468.

[133] *Klass and Others v Germany* [1978] ECHR 4, paras 48 and 68.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

ECHR if communications data was not accessed for the purposes for which it was retained.[134] This would also be a *prima facie* breach of the First[135] and Second[136] Data Protection Principles, especially since communications data might contains sensitive personal data which would therefore narrow the scope for compatible use.[137] Moreover, retaining communications data outside of what was permissible in *Klass* would not only violate Article 8 but also 'contravene the lawful processing requirement of the First Data Protection Principle'.[138]

(f) Appropriate remedy and the potential chaos that could ensue?

The claimants advocated for a suspended disapplication, which the High Court noted 'was a realistic and fair acknowledgement that, in this context, it cannot reasonably be expected that there should, immediately, be no legislation at all in place allowing retention of data that is needed to apprehend criminals or prevent terrorist attacks'.[139] The High Court acknowledged that whatever remedy it granted, it should not have the effect of 'immediately disapplying Part 4 of the 2016 Act, with the resultant chaos and damage to the public interest which that would undoubtedly cause in this country'.[140] The word 'chaos' is probably borrowed from the defendants, who argued that disapplication would be a recipe for chaos.[141]

A reason for the High Court not wishing to disapply Part 4 immediately is its assertion that there would be no legislation at all which permitted data retention.[142] This, however, is not true: the Budapest Cybercrime Convention[143] has been in force in the UK since 1 September 2011. This Convention principally concerns crimes committed via computer networks, but Article 14(2)(c) allows the UK to adopt measures to collect evidence of a criminal offence in electronic form. This does not appear to limit offences to those described in Articles 2–11 of the Cybercrime Convention, ie computer-related offences such as illegal interception, system interference etc. Additionally, Article 16 provides for data preservation, which is the alternative to data retention. This is not the only option available to the UK (see below). These points demonstrate that the High Court's position is effectively a strawman because immediate disapplication was not argued, and in any event, chaos would not ensue if Part 4 were to be immediately disapplied.

The High Court's reference to 'chaos' and 'damage' to the public interest is made without explaining how and why disapplying Part 4 of the IPA would have such a result. Such a position requires a critique. Prior to the DRIPA 2014, communications data retention had been voluntary (mandatory retention was repealed by section 105(1) two years after enactment) under section 102(1) of the Anti-terrorism, Crime and Security Act 2001 (although the Data Retention (EC Directive) Regulations of 2007 and 2009 required data retention to a lesser extent). Previous attempts at mandatory data retention, in the form of the draft Communications Data Bill was halted by the then partners to the Conservative Coalition, the Liberal Democrats.[144] There was no 'chaos' or 'damage' to the public

[134]Ben Emmerson QC and Helen Mountfield's Opinion to the ICO 19 June 2002, para 13.4(b), https://www.whatdotheyknow.com/request/127491/response/315758/attach/html/3/Counsels%20Opinion%20re%20The%20Telecommunications%20Regulations%201999%2019.6.02.pdf.html (accessed 4 November 2020).

[135]Ibid, para 9.7.

[136]Ibid, para 9.9.

[137]Article 29 Working Party 'Opinion 03/2013 on purpose limitation' 2 April 2013, para 25, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (accessed 4 November 2020).

[138]ICO 'Enforcement notice' 23 July 2012, para 9, http://breachwatch.com/wp-content/uploads/2012/08/Southampton-County-Council-Enforcement-Notice.pdf (accessed 4 November 2020).

[139]*Liberty*, above n 8, para 42.

[140]Ibid, para 46.

[141]Ibid, para 75.

[142]Ibid, para 42.

[143]Convention on Cybercrime, Budapest, 23 November 2001.

[144]T Brewster 'Nick Clegg "kills off snooper's charter"' 25 April 2013 https://www.silicon.co.uk/workspace/nick-clegg-kills-off-snoopers-charter-114390?inf_by=5ae711a1671db80f258b5b2d (accessed 4 November 2020).

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

interest prior to DRIPA 2014, when data retention was voluntary, nor when the draft Communications Data Bill was rejected. When the High Court in *Davis* disapplied section 1 of DRIPA 2014 (albeit delayed for eight months),[145] they felt it appropriate to give Parliament enough time to scrutinise and pass new laws,[146] not because of any chaos or damage that would ensue following immediate disapplication.

The High Court appeared to act on the assumption that if data retention obligations were immediately disapplied, there would be no communications data available to be accessed. This is untrue, as the Home Office even admits that telecommunications operators sometimes already retain data for 12 months,[147] and are willing to hand over usage and location data to the Government amidst the Coronavirus pandemic.[148] One of the biggest telecommunications operators in the world, Google, stores 'your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls'.[149] The legal basis for this retention is questionable,[150] but it highlights the fact that communications data could be accessed under section 61 of the IPA 2016 whether or not this data was in existence at the time, which means that telecommunications operators could be required to retain communications data on a 'forward looking basis'[151] irrespective of any retention obligation. This also reiterates the point made by former reviewer of terror legislation, David Anderson, that '[c]ommunications data are *frequently* used in the course of fast-moving operations, in which access will *often* be needed to data in *something close to real time*' (emphasis added),[152] thus the need for retention for 12 months weakens. Moreover, in the aftermath of the Madrid bombings,[153] 9/11[154] and 7/7, for the latter two, ISPs voluntarily preserved data.[155] With regard to the 9/11 preservations, Detective Inspector Mike Ford of the National Hi-Tech Crime Unit said 'I can assure you that the existence of the data has been of significant benefit and value'.[156] This establishes the ready availability of communications data without any retention obligations. It also ignores the fact that communications data is collected in bulk by the intelligence agencies under the IPA 2016, Part 6, Chapter 2. Notably, the USA does not currently have data retention laws,[157] but was still able to accumulate vast amounts of data, as Edward Snowden revealed. Additionally, the recent US Clarifying Lawful Overseas Use of Data Act (CLOUD Act) 'establishes a framework for permitting non-US law enforcement agencies to access communications data held by US operators [Microsoft, Google, Twitter, Facebook and others], and removes statutory prohibitions which might otherwise have prevented US operators from releasing the data'.[158] The hyperbolic language of the High Court is unhelpful, misleading and too uncritically succumbs to the Government's position.

[145] *Davis & Others*, above n 57, para 122.

[146] Ibid, para 121.

[147] Communications Data Code of Practice, above n 18, para 17.42.

[148] L Clarke 'UK could track mobile location data in coronavirus response' 20 March 2020, https://tech.newstatesman.com/security/uk-government-could-track-mobile-location-data-in-coronavirus-response (accessed 4 November 2020).

[149] M Spielkamp 'Google's private data retention' 1 July 2016, https://mobilsicher.de/uncategorized/googles-private-data-retention (accessed 4 November 2020).

[150] Ibid.

[151] Explanatory Notes to the Investigatory Powers Act 2016, para 177.

[152] D Anderson 'A question of trust, report of the Investigatory Powers Review' June 2015, para 9.24, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf (accessed 4 November 2020).

[153] European Digital Rights 'Shadow evaluation report on the Data Retention Directive (2006/24/EC)' 17 April 2011, para 13, https://www.edri.org/files/shadow_drd_report_110417.pdf (accessed 4 November 2020).

[154] All Party Parliamentary Internet Group 'Communications data: report of an inquiry by the All Party Internet Group' January 2003, para 182, https://www.cl.cam.ac.uk/~rnc1/APIG-report-commsdata.pdf (accessed 4 November 2020).

[155] I Brown 'Communications data retention in an evolving internet' (2010) 19 International Journal of Law and Information Technology 108.

[156] All Party Parliamentary Internet Group, above n 154, para 182.

[157] Electronic Frontier Foundation, 'Mandatory Data Retention: United States' https://www.eff.org/issues/mandatory-data-retention/us (accessed 4 November 2020).

[158] Brown, above n 118.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

The High Court referred to 'public interest' without clarification. Was it in reference to fighting serious crime and stopping terrorism? If this indeed was the case, the High Court did so without acknowledging that privacy, in and of itself, is a public interest,[159] which is specifically recognised in section 2(2)(d) of the IPA 2016. Privacy has a public value because it is necessary to the proper functioning of democratic political systems.[160] The then Labour Government acknowledged that 'the protection of privacy is in itself a public service'.[161] Privacy is a prerequisite for liberal democracies because it sets limits on surveillance by acting as a shield for groups and individuals.[162] Privacy underpins freedom of expression, religion, thought and conscious and assembly/association. It is not just an individual right, as data retention does not just affect individuals.[163] Not acknowledging the public interest privacy serves seriously underestimates the fundamental nature and importance of privacy.

(g) Not general and indiscriminate data retention?

When considering whether Part 4 of the IPA 2016 permitted general and indiscriminate data retention, reference was made to the Court of Appeal's refusal to hold that it was permitted under the DRIPA 2014.[164] The Court of Appeal's reasoning was unconvincing[165] and their semantic reasoning (see below) indicated what they would have held with regard to Part 4.[166] The claimants argued that Part 4 permitted general and indiscriminate data retention and should be referred to the ECJ, whereas the defendants argued that, read as a whole, Part 4 is compatible with EU law.[167]

The High Court deflected by noting that when ruling on general and indiscriminate data retention, the ECJ was referring specifically to Swedish law.[168] However, the ECJ's ruling referred to 'national legislation'[169] and acknowledged that the question was whether general and indiscriminate data retention per se[170] was compatible with EU law. Moreover, the Administrative Court referred only to traffic data,[171] whereas the ECJ also considered location data of all subscribers/users.[172] Thus, the ECJ's position is applicable to all EU Member States; Ni Loideain maintains that the ECJ were also considering UK law.[173] The High Court then summarised the ECJ's ruling by saying that Member States 'may adopt legislation which permits decisions to be taken for the *targeted* retention of data which is (a) sufficiently connected with the objective being pursued, (b) is strictly necessary and (c) proportionate' (emphasis added).[174] It appears that the High Court is cherry picking aspects of the ECJ's judgment. On the one hand, the ECJ was referring to Swedish law on the prohibition of general and

[159]*Riddick v Board Mills Ltd* [1977] QB 881, at 896.

[160]PM Regan *Legislating Privacy, Technology, Social Values and Public Policy* (The University of North Carolina Press, 1995).

[161]Cabinet Office 'Privacy and data-sharing: the way forward for public services' April 2002, para 52, https://ntouk.files.wordpress.com/2015/06/privacy-and-data-sharing-the-way-forward-for-public-services-2002.pdf (accessed 4 November 2020).

[162]AF Westin *Privacy and Freedom* (New York: Atheneum, 1967) p 24.

[163]M White 'The Privacy International case in the IPT: respecting the right to privacy?' 14 September 2017, https://eulawanalysis.blogspot.com/2017/09/the-privacy-international-case-in-ipt.html (accessed 4 November 2020).

[164]*Tom Watson and Others v Secretary of State for the Home Department*, above n 14, paras 22–26.

[165]M White 'Data retention is still here to stay, for now…' 5 February 2018, https://eulawanalysis.blogspot.com/2018/02/data-retention-is-still-here-to-stay.html (accessed 4 November 2020).

[166]M White 'Britain's mass surveillance regime is directly opposing human rights' 23 April 2018, https://theconversation.com/britains-mass-surveillance-regime-is-directly-opposing-human-rights-93323 (accessed 4 November 2020).

[167]*Liberty*, above n 8, para 120.

[168]Ibid, para 121.

[169]*Tele2 Sverige AB and Watson and Others*, above n 5, para 134(1).

[170]Ibid, para 50.

[171]Ibid, para 51.

[172]Ibid, para 62.

[173]N Ni Loideain 'Investigatory powers and human rights law' in L Edwards (ed) *Law, Policy and the Internet* (Oxford: Hart Publishing, 2019) p 177.

[174]*Liberty*, above n 8, para 124.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

indiscriminate data retention, and on the other, was referring to all Member States for targeted retention (which in and of itself implicitly rules out general and indiscriminate data retention for all Member States).

The High Court held that the ECJ's judgment did not require more detailed factors as it would be impracticable and unnecessary to set out in detail in legislation the range of factors to be applied, ie matters such as national security, public safety and serious crime.[175] It is unclear why the High Court refers to public safety; though the ECJ does refer to serious threats to public security, this, however, is with regard to the links between the measure and objective evidence.[176] The High Court did not explain why it would be impracticable and unnecessary to set out in detail the range of factors to be applied, considering the ECJ observed that national law must be clear and precise,[177] which Part 4 is not.[178] This also raises issues under the ECHR. The ECtHR has ruled that it is essential to have clear, binding[179] and detailed rules 'especially as the technology available for use is continually becoming more sophisticated'.[180] This is because, given the technological advances since the 1970s, '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'.[181] What the High Court considered unnecessary and impracticable are requirements of both European Courts, with the ECtHR taking extra steps to explain why.

The High Court held that the combination of the scope and application of data retention measures and the minimum safeguards are designed to achieve effective protection against the risk of misuse of personal data.[182] Granted this echoes the ECJ's position, it overlooks the ECtHR's in that the mere storing of data relating to private life amounts to an interference with Article 8, and the subsequent use has *no bearing* on that finding.[183] The misuse of personal data is secondary to it being generated and retained. The High Court distinguished the IPA 2016 from Swedish law in that the former does not 'contain a blanket requirement requiring the general retention of communications data'.[184] This is a semantic argument of 'distinguishing a catch all power, and a power that can catch all, which of course, in any event, amount to the same thing'.[185] The High Court relied on the statement that the Secretary of State will only issue a retention notice if it is necessary and proportionate as being in line with EU law.[186] This, however, directly contradicts a previous ruling on DRIPA 2014 (which too had the requirements of necessity and proportionality)[187] in which both parties in that case accepted it permitted a 'general retention regime'.[188] This was partly due to the secrecy of the contents of a retention notice[189] which is repeated in section 95(2)-(4) of the IPA 2016.

The High Court then argued that it would be difficult to conceive how the tests of necessity and proportionality could require the retention of all communications data because of the wording of 'all data' in the IPA 2016.[190] This, again, contradicts a previous ruling in that the High Court accepted that DRIPA 2014 permitted a 'general retention regime' which included the use of 'all data'[191] and that

[175]Ibid, para 124.
[176]*Tele2 Sverige AB and Watson and Others*, above n 5, para 111.
[177]Ibid, para 109.
[178]Cobbe, above n 68, at 19.
[179]*Valenzuela v Spain* (1999) 28 EHRR 483, para 60.
[180]*Roman Zakharov v Russia*, above n 127, para 229.
[181]*Szabo and Vissy v Hungary* (2016) 63 EHRR 3, para 53.
[182]*Liberty*, above n 8, para 125.
[183]*S and Marper v UK* (2009) 48 EHRR 50, para 67.
[184]*Liberty*, above n 8, para 127.
[185]White, above n 165.
[186]*Liberty*, above n 8, para 128.
[187]*Davis & Others*, above n 57, para 47.
[188]Ibid, para 65.
[189]Ibid, para 64.
[190]*Liberty*, above n 8, para 129.
[191]*Davis & Others*, above n 57, para 47.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

'the retention notices issued under it may be as broad in scope as the statute permits, namely a direction to each CSP to retain all communications data for a period of 12 months'.[192] The High Court's reasoning in *Liberty* acts on the assumption that surely the UK would not do such a thing. However, a 'power on which there are insufficient legal constraints does not become legal simply because those who may have resort to it, exercise self-restraint. It is the potential reach of the power rather than its actual use by which its legality must be judged'.[193] This is precisely what Cobbe argues, stating that:

> Retention notices may be tailored to an extent, including by requiring that only data which meets a certain description or is from a certain time period is retained. But section 87 does allow for ISPs to be required to retain 'all data' indiscriminately, without differentiation, limitation, or exception, and without clear safeguards for data subject to professional confidentiality.[194]

It has been argued that section 87(2)(a) and (b) theoretically allows for the possibility that 'all operators in the UK [being] required to retain all data of users and subscribers'[195] and should be treated as a blanket and indiscriminate power.[196] In *Liberty v UK* the UK Government accepted that section 3(2) of the Interception of Communications Act 1985 allowed 'in principle, any person who sent or received any form of telecommunication outside the British Islands during the period in question could have had such a communication intercepted'.[197] The ECtHR regarded this power as unfettered[198] and not 'in accordance with the law'[199] despite there being requirements of necessity[200] and a duty to take into account whether other means could be utilised to gain the information.[201] This demonstrates that adding 'necessary' and 'proportionate' in the terminology of a power does not guarantee its compliance with the ECHR. The High Court's reasoning also highlights yet another misinterpretation of EU law, in that the ECJ did not rule that general and indiscriminate data retention would be unlawful because it can be required, but because it can be provided. The IPA 2016 does not require general and indiscriminate data retention, but it makes that option possible. This reiterates the point that a law should be judged on its possibility and not on the assumed good faith of those who exercise it. Moreover, the High Court assumed that Part 4 of the IPA 2016 would only be unlawful if it did require a 'catch all' power. This is incorrect; the *Liberty v UK* case highlights that unlawfulness was found even though the measure did not concern a single communication within the UK. Additionally, in *S and Marper v UK*, the ECtHR ruled that blanket and indiscriminate biometric data retention of suspects violated Article 8.[202] This demonstrated that general and indiscriminate powers need not affect everyone (just a section of people) to be considered unlawful.

The High Court then incorrectly claimed that section 87(2)(b) of the IPA 2016 relates to 'a description of data' and not simply to 'all data'.[203] The correct construction of section 87(2)(b) refers to '*any* description of data', meaning any or all data could be retained, and not *a* description of data. This construction underestimates the breadth of what can be retained. The High Court made the same error when it came to telecommunications operators, in that a retention notice may relate to 'a particular operator or to a description of operators'.[204] Section 87(2)(b) actually refers to 'any' description

[192]Ibid, para 64.
[193]*Beghal v Director of Public Prosecutions* [2015] 3 WLR 344, para 102.
[194]Cobbe, above n 68, at 19.
[195]M White 'Protection by judicial oversight, or an oversight in protection?' (2017) 2(1) Journal of Information Rights, Policy and Practice 26.
[196]Ibid, at 25; Cobbe, above n 68, at 18; Murray, above n 92, at 161.
[197]*Liberty and Others v UK* (2009) 48 EHRR 1, para 64.
[198]Ibid.
[199]Ibid, para 70.
[200]Ibid, para 18.
[201]Ibid, para 21.
[202]*S and Marper*, above n 183, paras 125–126.
[203]*Liberty*, above n 8, para 129.
[204]Ibid.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

of operators. The suggestion here is that if a retention notice is issued to one telecommunications operator, because section 87(2) 'list[s] the elements which may be used when delineating the content and scope of a retention notice so as to satisfy the necessity and proportionality tests in any particular case',[205] this would be human rights compliant. However, when this is examined further, the problematic approach of the High Court becomes clear. Using the example of BT, which has over nine million broadband subscribers,[206] would a retention notice requiring BT to retain all the communications data of its subscribers be considered necessary and proportionate by the High Court? After all, BT is but one telecommunications operator, and thus could not retain communications data on every UK broadband subscriber, and therefore the requirement would not be general and indiscriminate, according to the High Court. Another example is Facebook, which dominates the social media sphere, owning Facebook, Facebook Messenger, WhatsApp and Instagram which rank 1st, 3rd, 4th and 6th respectively for the most used social networks in the UK.[207] The percentage of people aged 18 or over in the UK who use Facebook is 79%, with Facebook Messenger tallying 68%, WhatsApp 58% and Instagram 41%.[208] The exact number of the population in the UK as a whole that use Facebook and its various subsidiaries is not clear, but the Code of Practice indicates that it may not (meaning that it can) 'be necessary and proportionate to retain data in relation to all communications services provided by a company'.[209] This demonstrates that if it was deemed necessary and proportionate, Facebook and all its subsidiaries, which is utilised by a substantial portion of the adult UK population, could retain all communications data associated with use of its services. This does not even consider the use of Facebook's services by those under the age of 16[210] and the fact that retention notices have extraterritorial effect through section 97 of the IPA 2016. As of November 2018, the Home Office only admitted issuing fewer than 25 retention notices under section 87,[211] which could still cover the vast majority of the UK population.[212] However, this mass retention (which is not necessarily all encompassing) is as much a problem for the ECJ as it is for the High Court, for example, in relation to geographical data retention,[213] as *S and Marper* demonstrates that 'data retention measures that are general and indiscriminate within a group can still be unlawful'.[214]

The High Court next referred to the 12-month retention limit,[215] but this only serves to highlight the constant inference that retention notices will be renewed on a yearly basis. The High Court also referred to matters to which the Secretary of State must have regard in section 88(1), such as the benefits of the notice, number of users affected, costs etc, as well as taking reasonable steps to consult the relevant telecommunications operator (see section 88(2)). As to the former, the Secretary of State could still issue the intended retention notice despite having regard to those matters, and as to the latter, there is no obligation to actually consult a telecommunications operator.

[205]Ibid.

[206]BT 'Annual Report & Form 20-F' 2018, p 53 https://www.bt.com/bt-plc/assets/documents/bt-plc-financial-results/annual-reports/2018-bt-plc-annual-report.pdf (accessed 5 November 2020).

[207]A Battisby 'The latest UK social media statistics for 2018' 2 April 2018 https://www.avocadosocial.com/the-latest-uk-social-media-statistics-for-2018/ (accessed 5 November 2020).

[208]Ibid.

[209]Communications Data Code of Practice, above n 18, para 17.30.

[210]BBC Technology 'Under-age social media use "on the rise", says Ofcom' 29 November 2017 https://www.bbc.com/news/technology-42153694 (accessed 5 November 2020).

[211]See https://www.whatdotheyknow.com/request/526533/response/1271975/attach/3/attachment.pdf (accessed 5 November 2020).

[212]J Cobbe 'According to the Home Office, "fewer than 25" telcos or postal operators are or have been subject to retention notices under s 87 IPA 2016. That's still a lot – "fewer than 25" companies could cover the vast majority of the UK population' Tweet of 6 December 2018, 7:04 pm.

[213]White, above n 195, at 36.

[214]White, above n 11.

[215]*Liberty*, above n 8, para 130.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

The High Court next considered the role of JCs in approving retention notices based upon the Secretary of State's conclusions,[216] ie 'in deciding whether to approve a decision to issue a warrant, the Judicial Commissioners will ask themselves whether *the Secretary of State's decision* to issue a warrant' (emphasis added) is necessary and proportionate.[217] This is problematic, as there is 'no obligation on the Secretary of State to make a full and frank disclosure and therefore, the [Commissioners] … could be misled (accidently or deliberately)'.[218] The JCs could therefore be 'given a summary [of] a summary of a summary of a summary of a summary of the original intelligence case'.[219] The ECtHR has ruled 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'.[220] This is currently not an obligation under the IPA 2016.

The High Court then referred to the fact that JCs apply the principles of judicial review to authorisations.[221] The issue of whether the JCs will apply *Wednesbury* principles has been subject to debate.[222] The IPC has indicated that when human rights issues arise, the necessity and proportionality tests of the ECHR and EU law will apply instead of *Wednesbury*.[223] This statement was only advisory, and thus not a true safeguard,[224] and therefore the JC's role is not one of genuine independent oversight.[225] Additionally, the IPC and JC's independence is threatened not only by the executive/legislature, but by *themselves*;[226] this in turn would fail the test of independence required by the ECHR and EU law. It also raises an interesting question: when there is recourse to the IPA 2016, when would there *not* be human rights issues for *Wednesbury* to apply? The IPC did not elaborate on this, leaving the situation unsatisfactorily unclear.

The High Court next examined the general duties of JCs under section 2 of the IPA 2016.[227] The first of these concerns having regard to whether there are less intrusive measures to achieve the objective. It is submitted that there is one such measure: data preservation. But that is not possible under the IPA 2016 (unless one considers section 61 a form of preservation). The second duty concerns the level of protection provided to sensitive information, which is a much narrower category than the 'sensitive/special personal data' found within Article 9 of the General Data Protection Regulation, as it includes only legally privileged material, journalistic sources, communications with Members of Parliament etc. This is problematic, as the JCs cannot have regard to this sensitive information because – as noted by the Bar Council and Law Society – the problem with bulk communications data retention is that it does not prevent legally privileged data from entering the 'pool' in the first place.[228] This was a position the defendants implicitly accepted,[229] and is the position of the ECJ.[230] Jessica Sobey has argued that '[k]nowing who a lawyer contacts, when the contact was made and even where the point of contact was in geographical terms at the time, can be enough to represent a material breach of

[216]Ibid, para 133.

[217]IPCO 'Approval of warrants, authorisations and notices by judicial commissioners' Advisory Notice 1/2018 (8 March 2018), https://ipco.org.uk/docs/20180403%20IPCO%20Guidance%20Note%202.pdf (accessed 5 November 2020). See also P Scott 'Hybrid institutions in the national security constitution: the case of the Commissioners' (2019) Legal Studies 452.

[218]White, above n 195, at 30. For an analysis that makes it clear the JCs have been deliberately misled, see also M White 'The right to know – a human rights analysis of notifications under the Investigatory Powers Act' (forthcoming).

[219]White, above n 195, at 30–31.

[220]*Roman Zakharov v Russia*, above n 127 para 281.

[221]*Liberty*, above n 8, para 133.

[222]White, above n 195, at 26.

[223]IPCO, above n 217.

[224]White, above n 11.

[225]Scott, above n 217, at 453.

[226]See generally, for discussion on IPC/JC independence, White, above n 126.

[227]*Liberty*, above n 8, para 133.

[228]Law Society and Bar Council, 'Investigatory Powers and Legal Professional Privilege' (2015), https://gofile.io/d/DXUZn0 (accessed 29 November 2020), at 32.

[229]*Liberty*, above n 8, para 184.

[230]*Digital Rights Ireland Ltd v Seitlinger and Others*, above n 78, paras 57–58; *Tele2 Sverige AB and Watson and Others*, above n 5, para 105.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

privilege'.[231] The Law Society and Bar Council argued that 'new legislation should prevent an obligation being placed on service providers to retain data relating to communications to or from users known to be professional legal advisers'.[232] This was a position endorsed by Advocate General Øe,[233] and perhaps something the High Court should have given more consideration to, irrespective of the actions of the claimant.[234] With regard to journalistic sources, the United Nations Educational, Scientific and Cultural Organization (UNESCO) stated that even when journalists encrypt content, they may neglect to encrypt the communications data, which means they still leave behind a digital trail when they communicate with their sources, thus making them identifiable.[235] Moreover, the ECtHR has stressed that where sensitive personal data is involved, it should attract 'a heightened level of protection'.[236] It is difficult to agree with the High Court that section 2 of the IPA 2016 provides a sufficient safeguard, when that Court is unwilling to consider the threats Part 4 poses to journalism and the legal profession, to name but a few.

The High Court next noted that telecommunications operators can refer a retention notice back to the Secretary of State, which would then require approval by the IPC,[237] and that Part 4 and section 2 of the IPA 2016 allow a range of factors to be taken into account before a retention notice is issued.[238] The High Court summarised Part 4 by saying that it did 'not think it could possibly be said that the legislation requires, or even permits'[239] a general retention regime. This opinion proves problematic when a series of questions are asked. Can the Secretary of State issue a general and indiscriminate retention notice if it is deemed necessary and proportionate? (It can, see above reference to n 209.) Can a JC approve this? Can this be approved by the IPC after a referral by the telecommunications operator? If the answer is yes, then what? This emphasises that all the factors to be considered do not change the operation of the power itself. If the answer is no, where does Part 4 expressly prevent this? What is stopping the Commissioners from authorising general and indiscriminate data retention (whether on all, or on a group) if it is considered necessary and proportionate? The answer is that there is nothing to prevent this, and this is an escapable fact to which the High Court refused to address. The High Court's position is not only incorrect, but also contradicts its previous position, and the High Court does not adequately explain (see below) this complete reversal. This issue is not a matter of whether general and indiscriminate data retention will occur, but importantly, *can it*. The ECtHR has maintained that it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power.[240] Thus it would be unlawful even if retention notices are approved by Commissioners.

The High Court justified its departure from its previous ruling on data retention by arguing that:

> Even if that assumption were to be applied in this case, it is plain from the analysis set out above, that the 2016 Act does not permit the general and indiscriminate retention of communications data. In any event, we would add that the issue of whether a UK enactment is inconsistent with EU legislation is not to be determined by evidence from either party as to how the domestic

[231]J Sobey 'Legal professional privilege under fire' (2016) 180 Criminal Law & Justice Weekly 12 https://web.archive.org/web/20160923151907/http://www.halsburyslawexchange.co.uk/legal-professional-privilege-under-fire/ (accessed 5 November 2020).

[232]Law Society and Bar Council, above, n 228, at 32.

[233]Opinion of Saugmandsgaard Øe in *Tele2 Sverige AB and Watson*, above n 4, para 212.

[234]*Liberty*, above n 8, para 184.

[235]United Nations Educational, Scientific and Cultural Organization 'Protecting journalism sources in the digital age' 2017, p 26 https://unesdoc.unesco.org/ark:/48223/pf0000248054 (accessed 5 November 2020).

[236]*Catt v UK* [2019] ECHR 76, para 112.

[237]*Liberty*, above n 8, para 134.

[238]Ibid, para 135.

[239]Ibid, para 134.

[240]*Roman Zakharov v Russia*, above n 127 para 230.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

> scheme is operated in practice or might be operated. Instead, the issue is an objective question of law which turns on the proper interpretation of the two pieces of legislation.[241]

The High Court essentially argued that even if its previous ruling was correct, the IPA 2016 is somehow different from DRIPA 2014 – despite the relevant wordings being identical –without explaining why it should be construed differently. Remarkably, the High Court decided that it was not important how the law might be or is operated based on evidence, but upon this notion of the 'proper interpretation' of an 'objective question of law'. What does this mean? If the High Court is hiding behind the notion of objectivity, why is it that it 'thinks' Part 4 is not a general retention regime, whereas the DRIPA 2014 did permit this? Does 'proper interpretation' include overlooking the relevant ECtHR jurisprudence? The ECtHR not only considers measures applying the law, but the law itself,[242] in consistently holding that:

> [T]hat the *mere existence of laws and practices which permitted and established a system for effecting secret surveillance of communications* entailed a threat of surveillance for all those to whom the legislation *might b*e applied. This threat necessarily affected freedom of communication between users of the telecommunications services and thereby amounted in itself to an interference with the exercise of the applicants' rights under Article 8, *irrespective of any measures actually taken against them* (emphasis added).[243]

The High Court's position is in contrast with that of the ECtHR in that the lawfulness of secret surveillance can be judged either in abstracto or where an individual can claim to be an actual subject of surveillance. With the former, a risk of being subject to surveillance need not be demonstrated; with the latter, only a potential risk need be demonstrated.[244] The High Court also overlooked the possibility of secret interpretations of the law,[245] of which the UK's intelligence agency has already been found guilty.[246]

Whether retention notices apply to all or one telecommunications operator, to retain all or some communications data, this permits the 'automatic storage for six months of clearly irrelevant data' which 'cannot be considered justified under Article 8'.[247] This demonstrates that even a six-month retention period is unacceptable to the ECtHR, which highlights the problem with the 12-month retention period. This position is strengthened by the Opinion of Advocate General Øe, where he noted that '[t]he disadvantages of general data retention obligations arise from the fact that the *vast majority of the data retained will relate to persons who will never be connected in any way with serious crime*' (emphasis added).[248]

(h) The amendments

The Data Retention and Acquisition Regulations 2018[249] amend the IPA 2016 by inserting a new section 60A, which provides the power for the Investigatory Powers Commissioner to grant authorisations to obtain communications data. Section 60A(7)(b) permits communications data to be obtained for 'the applicable crime purpose'. This is defined in s 60A(8) as meaning:

[241] *Liberty*, above n 8, para 136.
[242] *Handyside v UK* (1976) 1 EHRR 737, [1976] ECHR 5, paras 47–51.
[243] *Roman Zakharov v Russia*, above n 127, para 168.
[244] Ibid, para 171.
[245] G Smith 'From oversight to insight – hidden surveillance law interpretations' 9 November 2018, https://www.cyberleagle.com/2015/11/from-oversight-to-insight-hidden.html (accessed 5 November 2020).
[246] *Liberty and Others v Secretary of State for Foreign and Commonwealth Affairs and Others* [2015] 3 All ER 212, para 32.
[247] *Roman Zakharov v Russia*, above n 127, para 255.
[248] Opinion of Saugmandsgaard Øe in *Tele2 Sverige AB and Watson*, above n 4, para 252.
[249] SI 2018/1123.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

(a) where the communications data is wholly or partly events data, the purpose of preventing or detecting serious crime;
(b) in any other case, the purpose of preventing or detecting crime or of preventing disorder.

This allows events data to be accessed for serious crimes, whereas entity data can be accessed for regular crime and disorder. Similarly, the 2018 amending Regulations amend section 87 of the IPA 2016 by inserting section 87(10A), which includes an 'applicable crime purpose' for a retention notice which has the same meaning as in section 60A(8). Thus, the threshold for retaining entity data is lower than that for events data.

Criticisms of this definition of serious crime, such as the 2018 amending Regulations failing to satisfy the requirements of *Digital Rights Ireland* by creating 'precisely defined serious offences', will not be set out in detail here.[250] However, it is important to note that, as argued above, entity data not only falls within the scope of EU law and the ECJ's judgments on data retention, the definition of entity data in the IPA 2016 confirms this. This is contrary to EU law; the ECtHR in *Big Brother Watch* stated:

> It is therefore clear that domestic law, as interpreted by the domestic authorities in light of the recent judgments of the [ECJ], requires that any regime permitting the authorities to access data retained by CSPs limits access to the purpose of combating 'serious crime'… As the Chapter II regime permits access to retained data for the purpose of combating crime (rather than 'serious crime') …it cannot be in accordance with the law within the meaning of Article 8 of the Convention. Accordingly, the Court finds that there has been a violation of Article 8 of the Convention.[251]

Whilst the ECtHR also found a violation of Article 8 because the Regulation of Investigatory Powers Act 2000 lacked authorisation by a court or an independent administrative body, it emphasised that where there is a conflict between domestic and law and EU law, the latter has primacy.[252] Allowing entity data to be retained for the purpose of 'preventing or detecting crime or of preventing disorder' is on its own merits a separate conflict between UK and EU law. Like the ECJ, the ECtHR did not distinguish between the types of communications data and confined its judgment to *any* data retained by communication service providers. Therefore, failing to confine the retention and access to retained data to serious crimes cannot be said to be 'in accordance with the law' within the meaning of Article 8. This would also demonstrate that purposes such as miscarriages of justice (see above) and the amendments to section 22 of the Regulation of Investigatory Powers Act 2000[253] would be contrary to EU law and the ECHR.

Additionally, in *Big Brother Watch*, the ECtHR stated that '[n]o interference can be considered to be "in accordance with law" unless the decision occasioning it complies with the relevant domestic law'.[254] The 2018 amending Regulations were made under section 2(2) of the European Communities Act 1972 and paragraph 4(3) of Schedule 7 to the IPA 2016. However, Schedule 7 applies to codes of practice rather than regulations. The correct legal basis on which to make regulations by way of statutory instrument (which is what the 2018 amending Regulations are) is via section 267(1)(a) of the IPA 2016. Therefore, the legal basis on which 2018 amending Regulations are created is not legally sound. Moreover, as noted above, the definition of entity data within the IPA 2016 places it within the scope of EU law and the ECJ's judgments; therefore, the 2018 amending Regulations are ultra vires the IPA 2016. In this instance, the UK has not observed its own laws, first, by creating regulations on an incorrect legal basis, and second, by said Regulations being ultra vires their parent

[250] A fuller critique can be found in White, above n 121.
[251] *Big Brother Watch and Others*, above n 62, paras 467–468.
[252] Ibid, para 466.
[253] By the Data Retention and Acquisition Regulations 2018, reg 3, which added s 22(2A), which includes 'prevention or detection of crime or of preventing disorder'.
[254] *Big Brother Watch and Others*, above n 62, para 465.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

statute with regard to entity data. The UK's failure to observe its own laws would also violate Article 8.[255] Finally, the Code of Practice notes that the IPA 2016 'provides that persons exercising any functions to which this code relates must have regard to the code, although *failure to comply with the code does not, of itself, make a person liable to criminal or civil proceedings*' (emphasis added).[256] This makes it clear that the Code of Practice is not binding, which again is contrary to what the ECtHR has established with regard to measures of secret surveillance.

Additionally, Regulation 5 set up the Office for Communications Data Authorisations (OCDA). However, the OCDA does not deal with all communications data requests (as the IPC still deals with some). The OCDA is also insufficiently independent, given the lack of transparency regarding its appointments. This would ultimately fall foul of the ECHR and EU law,[257] highlighting that even with changes, they are still insufficient.

Conclusions

This paper considered whether the High Court's ruling that Part 4 of the IPA 2016 was incompatible with EU law is a victory for privacy rights. In making this assessment, it was demonstrated that there were many flaws in the approach of the High Court that made its ruling not only inconsistent or incompatible with EU law, but also with the ECHR. The High Court's failure to consider the ECHR made it clear that the Court's judgment failed to promote a human rights compliant retention regime.

This ruling has, in effect, permitted the UK to continue with general and indiscriminate retention of communications data and contents due to the High Court's narrow and flawed interpretation of both these elements. The High Court has also allowed a disparity in protection of two different types of communications data – entity and events data – by stating that the former does not fall within the ambit (and thus, in contravention) of EU law, when in fact it does. This also highlighted that the High Court erroneously placed entity data outside scope of EU law and *Tele2 and Watson*. The High Court placed entity data outside the safeguards of *Tele2 and Watson* without even considering the ECHR. The High Court was also too accepting of the defendant's claim that disapplication of Part 4 would lead to 'chaos' and 'damage', when in reality much communications data would still be readily available and accessible. The High Court overlooked the lack of independence on part of the IPC and JC which was at the heart of both the ECtHR and ECJ's rulings. The High Court also too readily accepted national security (which, according to Advocate General Campos Sánchez-Bordona, cannot justify general and indiscriminate retention,[258] the ECJ generally agrees)[259] as a trump card, despite it not being clear for ECHR purposes. The High Court also too hastily accepted other purposes (eg miscarriages of justice) for retention that are incompatible with EU law and with the ECHR (for lacking foreseeability and failing to adhere to the primacy of EU law, and for being contrary to *Klass and Others*). Any inconsistencies with the ECHR should theoretically also make the IPA 2016 and the High Court's ruling inconsistent with the Charter.

The amendments to the IPA 2016 made by the 2018 amending Regulations do not remedy the problems that have been highlighted in the High Court's judgment; if anything it is the High Court's judgment that has enabled those amendments to a certain degree. The 2018 amending Regulations permit differing purposes for retention and access to events and entity data, which is contrary to EU law, and

[255] *Mustafa Sezgin Tanrikulu v Turkey* [2017] ECHR 669, paras 60 and 64–65.

[256] Communications Data Code of Practice, above n 18, para 1.8.

[257] White, above n 126, at 529.

[258] Case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service* [2020] EUECJ C-623/17_O, Opinion of Campos Sánchez-Bordona para 45.

[259] Case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service* [2020] WLR(D) 573, para 83(2); Case C-511/18, *La Quadrature du Net and Others* [2020] WLR (D) 572.

https://doi.org/10.1017/lst.2020.35 Published online by Cambridge University Press

would be a violation of Article 8 of the ECHR. The way in which the amending Regulations were drafted is not the fault or responsibility of the High Court, but they do not even comply with their parent legislation, the IPA 2016, in terms of the correct legal basis for their existence. In any event, the High Court's judgment set in motion for the 2018 amending Regulation to remove entity data (in that serious crime is not a necessary threshold) from the scope of EU law and *Tele2 and Watson*, contrary to the actual definition of entity data found within the IPA 2016 itself.

The High Court's ruling is not a victory for privacy rights when it is not even considered to constitute an element of the public interest. It is also not a victory for privacy rights because the points on which the defendants were ruled against were already in the process of being (unlawfully) amended. It is not a victory for privacy rights because the substance of the High Court's ruling is heavily flawed, and although the IPA 2016 was found to be in violation of EU law, any notion of victory appears hollow as it is symptomatic of the 'minimalist response of the UK to European rulings on privacy generally and state surveillance specifically'.[260] It is also not a victory in the wider context of data retention at the EU level when the Council of the European Union still considers that data retention is necessary for fighting crime and that subscriber data is outside the scope of the ECJ's rulings.[261] As of 29 November 2018, Liberty had successfully been permitted to judicially review the rest of the IPA 2016,[262] however, this resulted in the High Court ruling that the IPA 2016 contained sufficient safeguards.[263] This is to be appealed,[264] so only time will tell whether this will be more of a victory than the ruling on data retention.

[260]L Woods 'Automated number plate recognition: data retention and the protection of privacy in public places' (2017) 2 (1) Journal of Information Rights Policy and Practice 1.

[261]Council of the European Union 'Council Conclusions on improving retention of data for the purpose of fighting crime effectively' 27 March 2019, paras 6 and 4 http://www.statewatch.org/news/2019/apr/eu-council-data-retention-draft-conclusions-7833-19.pdf (accessed 5 November 2020).

[262]Liberty 'Liberty wins the right to challenge bulk surveillance under snoopers' charter' 29 November 2018, https://www.libertyhumanrights.org.uk/?s=Liberty+wins+the+right+to+challenge+bulk+surveillance+under+snoopers%E2%80%99+charter (accessed 5 November 2020).

[263]*Liberty v SSHD and SSFCA* [2019] EWHC 2057 (Admin).

[264]BBC 'Rights group loses mass surveillance appeal in High Court' 29 July 2019, https://www.bbc.com/news/uk-49153593 (accessed 5 November 2020).

Cite this article: White M (2021). Is the incompatibility of UK data retention law with EU law really a victory? *Legal Studies* **41**, 130–155. https://doi.org/10.1017/lst.2020.35