LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

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

About Liberty

Liberty (the National Council for Civil Liberties) is the UK's leading civil liberties and human rights organisation. Liberty works to promote human rights and protect civil liberties through a combination of litigation, lobbying, campaigning, and research.

Liberty's policy papers are available at
http://www.liberty-human-rights.org.uk/policy/

Contact

Corey Stoughton
Advocacy Director
Direct Line 020 7378 3667
Email: coreys@liberty-human-rights.org.uk

INTRODUCTION

1. Liberty represents Mr Tom Watson MP in the case prompting this consultation, which challenges the compatibility of the Data Retention and Investigatory Powers Act 2014 ("DRIPA") with privacy rights recognised under EU law. The Court of Justice of the European Union ("CJEU") handed down its judgment on 21 December 2016 on the joined cases *Tele2 Sverige AB v Post-och telestyrelsen* (Case C-203/15) and *R (Watson) v Secretary of State for the Home Department* (Case C-698/15), specifying a number of EU law requirements a regime governing the retention and acquisition of communications data must meet in order to avoid violating individual privacy.

2. Nearly a full year later, on 30 November 2017, the Government published a proposed response to the CJEU's ruling and launched this public consultation.

3. Liberty welcomes the opportunity to respond to this consultation. However, we are concerned by the very slow response to the CJEU's clear finding that the UK's data retention and access regime is incompatible with fundamental rights. Urgent and serious change to protect people's privacy has been required by law for over a year. The Government should be long past weighing options; it should be implementing solutions.

4. Liberty is also deeply concerned that the Government's proposal addresses only some of the CJEU's judgment, choosing to ignore some aspects and misrepresenting others. It is wrong for the Government to launch a public consultation on proposals that seek to reject or circumvent express mandatory safeguards identified in a court judgment. Like everyone else, the Government must comply with the law. A public consultation cannot add or take away from the requirements of the law. Nor could a consultation provide legitimacy for proposals that do not satisfy requirements identified in a court judgment. In our response we cite key sections of the CJEU's judgment and relevant EU directives that make clear where the Government misrepresents or ignores them.

5. In the interests of protecting fundamental rights in the UK and upholding the adequacy of the UK's data laws to meet EU standards, the Government should implement serious reforms to the current data retention and acquisition framework in full compliance with the letter of the CJEU's judgment, and the important individual privacy rights that underlie that judgment. The current proposal contains some steps in the right direction but is, unfortunately, incomplete and inadequate. In this

response, Liberty focuses on those inadequacies so that the Government can move as quickly as possible to address them.

6. Liberty is presently engaged in litigation with the Government about whether the Investigatory Powers Act 2016, and in particular Part 4 of that Act, complies with the requirements established by *Watson*. Nothing in this submission isor is intended to be in any way inconsistent with Liberty's submissions in that litigation (which Liberty does not repeat, save where relevant to the matters raised by this consultation).

I. The Government's Proposed Definition of "Serious Crime" Creates Conflicting, Confusing, and Overbroad Standards For When Communications Data Can Be Retained and Acquired.

7. The CJEU's judgment found that the ePrivacy Directive, read in light of privacy rights protected by the Charter, (emphasis added)

   "*(…) must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access,* ***in the context of fighting crime, is not restricted solely to fighting serious crime*** *(…)*"

   in addition to requiring prior independent authorisation and retention of data within the European Union.[1]

8. The Government's response acknowledges this ruling, stating that it "proposes to amend the Act to impose a serious crime threshold in relation to the retention and acquisition of events data for criminal purposes."[2] But, rather than adopt the existing "serious crime" definition approved by Parliament and incorporated into the Investigatory Powers Act 2016 ("IPA"), the Government proposes a new definition not reflected in or recognisable in relation to any of the UK legal instruments that grapple with the notion of "serious crime."

[1] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970), p.2.

[2] Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017 (hereinafter, "Consultation Document"), p.15.

9. This proposed amendment would result in three different crime thresholds and two conflicting definitions of "serious crime" within the IPA scheme, risking legal confusion. Moreover, the definition the Government proposes makes the concept of "serious" crime so expansive that it does not serve as a real limit on the matters that justify retention of communications data, and thereby lowers the level of privacy protection below the already inadequate *status quo*.

A. The Proposal's Multiple, Conflicting Crime Thresholds Create Legal Confusion.

10. "Serious crime" is already defined in the IPA as conduct involving the use of violence, which results in substantial financial gain, or conduct by a large number of persons in pursuit of a common purpose; or an offence for which an adult could reasonably be expected to be sentenced to three years or more in prison.[3] This definition is very similar to that adopted in a predecessor statute, the Regulation of Investigatory Powers Act 2000.

11. With regard to accessing internet connection records ("ICRs"), the IPA introduces a second crime threshold of serious crime or *"*other relevant crime,"[4] which is defined as an offence for which an adult should be capable of being sentenced to twelve months or more in prison, or an offence which involves "*the sending of a communication"*.[5]

12. The Government's proposed amendment would introduce an "applicable crime" purpose, which has two interpretations: the first maintains the previous purpose of preventing or detecting any crime or preventing disorder; the second applies only if the data sought is *"*events data", in which case an entirely new "serious crime" definition would apply.[6]

[3] Investigatory Powers Act 2016, s.263.

[4] Investigatory Powers Act 2016, s. 62(5).

[5] Investigatory Powers Act 2016, s. 62(6).

[6] The Data Retention and Acquisition Regulations 2018 (Draft Statutory Instruments), amendment of section 61, p.3: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/663677/November_2017_IPA_Consultation_-_Draft_regulations_amending_the_IP_Act.pdf

13. The new “serious crime” threshold is defined as an offence for which an adult should be capable of being sentenced to six months or more in prison, an offence by a person who is not an individual, or an offence which involves the sending of a communication. This bespoke definition of “serious crime” sets a lower threshold than any of the IPA’s other crime thresholds and conflicts with the existing definition of “serious crime” in the IPA.

14. The new definition would add to an already over-complicated framework which would include two very different definitions of “serious crime,” as well as definitions of “other relevant crime” and “applicable crime” in relation to communications data. Such legal confusion is neither appropriate nor desirable.

B. <u>The Proposed New Definition of “Serious Crime” Would Unreasonably Erode Privacy Protections</u>.

15. The Government’s proposed definition of “serious crime” for the purposes of communication data sets the threshold so low it might well be interpreted as an effort to evade the CJEU’s ruling. It also strays far from the balance Parliament sought to strike between privacy and law enforcement needs in the IPA.

16. The CJEU’s judgment recognised the seriousness of the interference with fundamental rights incurred by the retention of and access to individuals’ communications data. The judgment clearly requires a serious crime threshold as a vital safeguard for access to all communications data.

17. The proposed new definition—that is, any offence for which an adult should be *capable* of being sentenced to six months or more in prison, an offence by a person who is not an individual, or an offence which involves “the sending of a communication”—is not a meaningful reform of the current unlawful framework. There are vanishingly few criminal offences that would not be, by this definition, considered “serious”. In a meeting at the Home Office regarding this consultation, we were told that the only offences not included in this definition would, in practice, be ‘summary offences’ (e.g., road traffic offences).

18. This amendment would clearly be inconsistent with, and evade the spirit of, the CJEU’s judgment, which was clear (emphases added):

"The interference entailed by such legislation in the fundamental rights enshrined in Articles 7 and 8 of the Charter is ***very far-reaching and must be considered to be particularly serious****."*[7]

"*Given the seriousness of the interference in the fundamental rights concerned (…)* ***only the objective of fighting serious crime is capable of justifying such a measure*** *(…)"*[8]

"Further, while the effectiveness of ***the fight against serious crime, in particular organised crime and terrorism,*** *may depend to a great extent on the use of modern investigation techniques, such an objective of general interest,* ***however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention*** *of all traffic and location data should be considered necessary for the purposes of that fight."*[9]

19. The new definition of "serious crime" expands the category far beyond the existing statutory definition – indeed, beyond any reasonable person's understanding of the term. As noted above, 'serious crime' in s. 263 of the IPA has already been defined as conduct involving the use of violence, that results in substantial financial gain, or is conducted by a large number of persons in pursuit of a common purpose; or an offence for which an adult could reasonably be expected to be sentenced to three years or more in prison.[10] Any serious crime related to child abuse or harassment, as well as any significant corporate crime, is already covered by this definition.

20. It is of particular importance that the powers cannot be used for an offence where an adult could not reasonably be expected to be sentenced to three years or more in prison. For example, s. 263 would not be satisfied in a case where a person is suspected of possessing cannabis for personal consumption (even though the maximum sentence for possession is 5 years). It cannot seriously be considered that the possession of cannabis for personal consumption ranks alongside the fight

[7] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 100

[8] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 102

[9] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 103

[10] Investigatory Powers Act 2016, s.263

against organised crime and terrorism in assessing the appropriate balance between public safety and individual privacy.

21. The new "serious crime" definition would apply to communications data acquisition under Part 3[11] and retention under Part 4.[12] Because this new definition of serious crime would apply to all of Part 3, it would appear to also change the meaning of the threshold on access to ICRs, making it lower than in the current IPA threshold.[13] Lowering privacy thresholds in response to a judicial ruling that finds that the UK's surveillance regime violates privacy rights is entirely inappropriate.

22. This reduction in privacy protection is particularly disturbing given that the existing low threshold for ICRs was already controversial during the passage of the IPA. As then-Shadow Home Secretary, Andy Burnham MP, noted during the debate:

"*I believe the threshold at which ICRs can be accessed must be higher. . . . I do not think it is necessary or proportionate for information held in ICRs to be accessed in connection with lower-level offences. Instead, I think* ***this threshold should be set at serious crime and that this should be defined in the Bill as an offence that attracts a maximum sentence of not less than three years in prison.***"[14]

[11] The Data Retention and Acquisition Regulations 2018 (Draft Statutory Instruments), Schedule 1, para. 21 (3), pp. 11-12 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/663677/November_2017_IPA_Consultation_-_Draft_regulations_amending_the_IP_Act.pdf

[12] The Data Retention and Acquisition Regulations 2018 (Draft Statutory Instruments), Retention of communications data, pp. 5-6 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/663677/November_2017_IPA_Consultation_-_Draft_regulations_amending_the_IP_Act.pdf

[13] Investigatory Powers Act 2016, s. 62(5).

[14] *Letter to the Home Secretary on the Investigatory Powers Bill* – Andy Burnham MP, 4th April 2016, http://andyburnhammp.blogspot.co.uk/2016/04/letter-to-home-secretary-on.html .

II. The Government's Proposal Does Not Satisfy the CJEU's Prohibition on General and Indiscriminate Data Retention for Purposes of Fighting Serious Crime.

23. The CJEU was explicit about the incompatibility of mass communications data retention with the right to privacy. In the consultation paper, the Government acknowledges and recites this aspect of the judgment:

    "(EU law) must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication."[15]

24. The CJEU's judgment stated that a *"generalised manner"* of retention "*provides for no differentiation, limitation or exception according to the objective pursued"* and thus affects all persons using specified services *"even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings."*[16]

25. The CJEU's judgment was clear that legislation that "*does not require there to be any relationship between the data which must be retained and the threat to public security"* is incompatible with Articles 7, 8 and 11 of the Charter of Fundamental Rights and *"cannot be considered to be justified, within a democratic society."*[17]

26. A data retention regime therefore requires a relationship between the specific data required for retention and a specific threat to public security. The CJEU's judgment allows for legislation permitting *"targeted retention"* of data as a preventative measure for the purpose of fighting serious crime where the persons concerned, categories of data retained, means of communication affected, and retention period are limited to what is strictly necessary.[18]

---

[15] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970), para. 112.

[16] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 105.

[17] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): paras. 106-107.

[18] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 108.

27. In discussing the rules governing access to retained data, the CJEU's judgment requires a highly specific level of individualised suspicion, holding that (emphasis added),

"access can, as a general rule, be granted, in relation to the objective of fighting crime, ***only to the data of individuals suspected of planning, committing or having committed a serious crime*** *or of being implicated in one way or another in such a crime."*[19]

28. Individualised suspicion where data is sought for the purpose of preventing or detecting crime is a clear requirement in law and is a general safeguard similarly required for use of investigatory powers in *Zakharov v Russia*[20] and *Szabó and Vissy v Hungary.*[21] The CJEU explicitly referred to this requirement in the context of access to communications data.[22]

29. The Government's proposal directly conflicts with the judgment and the right to privacy, based on the incorrect conclusion that "*we do not consider that the existing data retention regime is 'general and indiscriminate'".*[23] The Government's conclusion is based on a list of factors that the Secretary of State should take into account when issuing a data retention notice to a telecommunications operator under the Investigatory Powers Act 2016 (IPA). These factors include a consideration of the operator's services to which the notice should relate; *whether* it would be appropriate to restrict a notice by geography or to exclude groups of customers; and to link the notice clearly to the statutory purpose for which it is issued (e.g. for the prevention and detection of crime).

30. These very basic factors for consideration do not adequately address the requirement that an order for a telecommunications operator to retain people's

---

[20] *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [260].

[21] *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [71].

[22] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para.119-20.

[23] Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017 (hereinafter "Consultation Document"), p.14.

communications data for the purpose of ensuring that the State can later access it must be targeted. A targeted notice would require, at a minimum, a relationship between the individual's data retained and a specific threat to public security, not merely a general link to the prevention and detection of crime.

31. In its consultation paper, the Government has not acknowledged the requirement of individualised suspicion—even for access to retained communications data—and no amendments have been proposed to add this important safeguard into the IPA. It remains the case that communications data can be retained for the general purpose of preventing and detecting crime without any grounding in individualised suspicion, or even any requirement to meaningfully meet a requirement to be "targeted." This could mean that individuals' data could be retained without any reason to believe that they are implicated in a crime.

32. Moreover, a serious response to this aspect of the CJEU's judgment would contain *rules* limiting the scope of retention notices to ensure that they are targeted, not mere "factors" for consideration by a minister. A balancing of factors ultimately does not prevent the Government from violating individual privacy, including by mass retention of people's private communications data that has no direct connection to criminal activity. Indeed, a policy to *consider* whether a notice should be geographically targeted or *whether* it should exclude groups of people makes it clear that, as a default position, there is no restriction whatsoever on the ability to issue mass data retention notices, and that capturing all or most of the users of a service is to remain the rule rather than the exception. This is contrary to the CJEU's judgment, which explicitly stated that "*the system put in place by Directive 2002/58 requires the retention of data to be the exception.*"[24] When the legal right to privacy is implicated, it is simply not enough for the Government to reassure the public with vague promises about the "*practical effect of the regime.*"[25] An enforceable legal framework striking the right balance between privacy and security is required.

33. The Government's proposed amendments to the IPA scheme still permits Government to issue a retention notice relating to <u>all</u> communications data held by a telecommunications operator, resulting in the retention of innocent people's data

[24] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 104

[25] Consultation Document, p. 14.

where the Secretary of State is doing so for the purpose of preventing and detecting a broad range of crimes (see section 87(2)(b) of the IPA). None of the proposed amendments protect the communications data of Liberty or any similarly situated organisation or individual who is engaged in no wrongdoing nor even suspected of wrongdoing.

34. The Government's response to this rests mainly on non-binding reassurances that it will not use its powers fully in practice. Even if mere reassurances about practice were enough to satisfy legal obligations to respect privacy rights, which they are not, the Government's facts are not especially assuring. The only evidence the Government points to suggesting that retention notices are targeted is the fact that, of more than 700 telecommunications and postal operators it has engaged with in the last two years, fewer than 25 have been served a data retention notice. To the extent this statistic is meant to demonstrate that very little communications data is subject to retention notices, it is misleading. As an initial matter, it is only a description of the Government's use of its power so far, in the early stages of having acquired expanded retention powers in 2016.

35. More importantly, a small number of telecommunications operators hold the vast quantity of our communications data. The Government does not (in accordance with its "neither confirm nor deny" policy) disclose which 25 companies have been subject to retention notices. If the 25 telecommunications operators who have received retention notices include the UK's major mobile phone and internet service providers, then it matters little whether Government has served retention notices on any of the hundreds of smaller companies who rely on infrastructure provided by those larger ones. The definition of "telecommunications operator" is so broad it includes, for example, every café, hotel, or library that provides public wifi; every app developer; and every manufacturer of a toy or small home appliance that connects to the internet (as illustrated in the Draft Communications Data Code of Practice, paras. 2.1-2.12). These entities—and indeed most small and medium-sized internet service providers and mobile network operators—generally use the physical telecommunications infrastructure of a very small number of larger companies. Given the broad definition of "telecommunications operator" and the reality of the way telecommunications works, it is no wonder that only a small percentage of "telecommunications operators" are subjected to data retention notices.

36. Conversely, although the power to serve notices on these smaller companies exists, if such notices are served they will not be disclosed, and the existence of this power is in itself incompatible with EU law and the ECHR.

III. The Exemption for "Entity Data" Is Inconsistent with the CJEU's Judgment.

37. The Government's proposal erroneously suggests that the CJEU's judgment does not apply to a specific category of communications data it terms "entity data," and thus exempts that category of communications data from some of the critical privacy protections mandated by the judgment, including by allowing entity data to be accessed for any crime purpose (not limited to "serious crime") and allowing requests for entity data to be internally authorised by low-level staff.

38. The IPA defines a set of vague and overlapping sub-categories of communications data—including "systems data," "(relevant) communications data" (which may include "'entity data" and "events data"), "internet connection records," and "secondary data" or "equipment data" (which may include "identifying data" or "(related) systems data"). The Government's proposal seems to exploit the confusion created by these statutory definitions to avoid the full application of the CJEU's judgment.

39. The Government argues that "The CJEU judgment refers to only certain types of communications data – traffic data and location data, as defined in Directive 2002/58/EC ('the ePrivacy Directive')."[26] Subsequently, the Government argues, "the CJEU's judgment should be read as applying to 'events data' but does not apply to the retention or acquisition of 'entity data'",[27] as defined in the IPA. Based on this incorrect assertion, the draft Regulations do not limit requests for "entity data" to cases involving serious crime. *Any* potential criminal offence, no matter how minor, can be used as a basis to obtain entity data.[28] In addition, entity data can be obtained for non-criminal purposes, including the prevention of (non-criminal) "disorder", which is not a defined term. Requests for entity data may also be authorised at a lower level within public authorities.[29]

[26] Consultation Document, p.10.

[27] Consultation Document, p.11

[28] Home Office, *Communications Data: Draft Code of Practice* (Nov. 2017) para. 3.4.

[29] Home Office, *Communications Data: Draft Code of Practice* (Nov. 2017) para. 2.35.

40. The interpretation that the CJEU's judgment should apply only to traffic and location data—and that such data should be read exclusively as 'events data' rather than 'entity data' in the IPA—is plainly wrong, for the reasons detailed below.

A. The CJEU's judgment does not distinguish entity data from events data.

41. First, the CJEU drew no distinction between entity data and any other category of communications data in its judgment. Nor did the referring court (the Court of Appeal) in the Order for Reference. Nor did the Government suggest to the CJEU during the reference that it was only being asked to consider traffic data and location data. For example, the judgment of the Court of Appeal making the reference expressly explains that communications data "*fall into three broad categories" including "(1) subscriber data: information held or obtained by a communications service provider… in relation to a customer, for example their name, address and telephone number*."[30] And while the subcategories of "entity" and "events" data are outlined in Part 9, Chapter 2 of the IPA, they are not used, or in any manner substantively differentiated, in the frameworks for obtaining communications data outlined in Parts 3 or 4. There is, therefore, no basis in law for the Government's attempt to exclude "entity data" from the requirement for prior independent authorisation.

B. ***"***Entity data" is within the scope of the ePrivacy Directive.

42. Second, the Government's attempt to distinguish "entity data" turns on a presumption that the ePrivacy Directive, which the CJEU interpreted in order to arrive at its judgment, concerns "traffic and location data" and not "entity data." This argument misreads the ePrivacy Directive.

43. While the ePrivacy Directive does indeed define traffic data and location data in Article 2 ('Definitions'), the Directive is not restricted to these two subcategories of communications data. Article 1 of the ePrivacy Directive, headed 'Scope and Aim', is clear:

    1. *This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy,* ***with respect to the processing of personal***

[30] [2016] 1 CMLR 47 at [5].

data in the electronic communication sector *and to ensure the free movement of such data and of electronic communication equipment and services in the Community.*[31]

44. Article 3 of the ePrivacy Directive, headed 'Services concerned', provides:
    1. *This Directive shall* ***apply to the processing of personal data*** *in connection with the provision of publicly available* ***electronic communications services*** *in public communications networks in the Community.*[32]

45. The ePrivacy Directive, as stated in its title, applies to *"personal data and the protection of privacy in the electronic communications sector"* – it applies to communications data, not only select subtypes of data.

46. The ePrivacy Directive was amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 ('Data Retention Directive', now invalid). The CJEU's judgment acknowledges and indeed recites Article 1(2) of the Data Retention Directive, which addressed "Subject matter and scope" as follows (emphases added):

    "*This Directive* ***shall apply 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****. It shall not apply to the content of electronic communications (…)"*[33]

47. The CJEU specifically cites several Recitals of the ePrivacy Directive as relevant to its judgment, including the following (emphases added):

    "(7) In the case of public communications networks, specific legal, ***regulatory and technical provisions should be made in order to protect fundamental rights and freedoms*** *of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated* ***storage and processing of data relating to subscribers and users****."*[34]

[31] Directive 2002/58/EC ('the ePrivacy Directive'), Article 1(1)

[32] Directive 2002/58/EC ('the ePrivacy Directive'), Article 3(1)

[33] Directive 2006/24/EC, ('the Data Retention Directive), Article 1(2)

[34] Directive 2002/58/EC ('the ePrivacy Directive'), Recital 7

*"(26) 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 interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service (…) and for a limited time. Any further processing of such data (…) may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider (…)"*[35]

48. The CJEU's judgment confirms the scope of the ePrivacy Directive, which it says "*must be regarded as regulating the activities of the providers of such* (electronic communications) *services".*[36] The judgment further clarifies that the ePrivacy Directive *"applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies",* and continues (emphasis added):

    *"As confirmed in recital 21 of that directive, the aim of the directive is to prevent unauthorised access to communications, **including 'any data related to such communications',** in order to protect the confidentiality of electronic communications".*[37]

49. Finally, the CJEU's judgment stated:

    "*It follows from the foregoing that national legislation, such as that at issue in the main proceedings in Cases C-203/15 and C-698/15, falls within the scope of Directive 2002/58."*[38]

50. The CJEU did not find that only certain categories of communications data fall within the scope of the ePrivacy Directive, but rather that the national legislation in question fell clearly within the scope of the Directive.

[35] Directive 2002/58/EC ('the ePrivacy Directive'), Recital 26

[36] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 70

[37] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 77

[38] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 81

51. The CJEU's judgment also described, in detail, the fields of data with which it is concerned:

"The data which providers of electronic communications services must therefore retain makes it possible to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to establish the location of mobile communication equipment. That data includes, inter alia, the name and address of the subscriber or registered user, the telephone number of the caller, the number called and the IP address for internet services."[39]

52. Clearly, many of the data types described, and to which the judgment applies, fall within the subcategory of "entity data" under the IPA.

C. "Entity Data" includes location data, which is expressly covered by the CJEU judgment.

53. "Entity data" under the IPA includes location data, which is the express focus of the CJEU's judgment. "Entity data" is defined in section 261 of the IPA as follows (emphases added):

(3) "Entity data" means 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.

54. The definition is explicitly inclusive of location data. Entity data is personal data that identifies users and subscribers to a communications service. The definition of entity data in the IPA includes, in addition to identifying data, descriptive data which may refer to the entity's location. For example, entity data that identifies the subscriber to a line rental and broadband service includes the person's home address to which the

[39] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 98

service is provided. Thus, even on the basis of the Government's restrictive interpretation of the CJEU's judgment, it is quite clear that 'entity data' as defined in the IPA (i.e., as including location data) is within the scope of the CJEU judgment.

D. "Entity Data" May Include Other Significant Information Engaging Privacy Rights.

55. The definition of "entity data" is vaguely drafted, leaving people in the UK unsure about how it will be interpreted by the Government and the telecommunications operators in their bilateral discussions. By its plain language, however, the term covers 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. This information would be "entity data" because "entity data" includes "the services … to which the owner of the devices subscribes."[40]

56. From data about which apps a person has subscribed to or has downloaded, one could identify a broad range of private information about a person, including which bank a person uses and where her investments reside (by banking or investment services apps such as NatWest, etc.), what newspapers they read (e.g., MailOnline or Guardian apps), whether they have children (by any number of apps designed to educate or entertain small children or support parents of young children), a person's sexuality (by subscription to gay dating apps such as Grindr). There are even apps subscriptions which would reveal that a person is having, or is interested in having, an affair.[41]

57. For all of these reasons, there is no basis for the Government's presumption that "entity data" should be treated differently from other categories of communications data.

[40] Home Office, *Communications Data: Draft Code of Practice* (November 2017) para 2.24

[41] For example, the "Ashley Madison" application: see https://itunes.apple.com/us/app/ashley-madison/id359478823?mt=8.

IV. National Security Interests Do Not Provide a Blanket Exemption from EU Law and Privacy Rights.

58. The consultation does not seek views on the application of the judgment to national security cases or the agencies with national security functions. Nevertheless, it is clear that the Government's position on this is not lawful. DRIPA was national security legislation, and expressly included national security as a basis for retention. EU law applies because data retention rules (and associated access arrangements) place requirements on companies who often operate across the EU. EU law has harmonised the rules that may be applied to such companies. EU law applies, even in "the national security context" (a vague term which the government does not seek to define). The UK has repeatedly run and invariably lost such arguments in the CJEU. The most recent example is *ZZ v Secretary of State for the Home Department* [2011] EWCA Civ 440; *ZZ (France) v Secretary of State for the Home Department* (C-300/11), reported in EU:C:2013:363; *ZZ (France) v Secretary of State for the Home Department*, [2015] EWCA Civ 987, [2017] EWCA Civ 133.

59. The Government's "national security" loophole is so broad that it even permits public authorities other than MI5, MI6 or GCHQ, including local councils and police, to avoid important privacy safeguards—including the requirement of independent authorisations for requests to access private communications data—by linking their purpose to national security or the economic well-being of the UK (when linked to national security).[42]

60. The breach of EU law in failing to comply with the judgment in national security cases is so obvious and flagrant that it risks giving rise to substantial financial liabilities for HM Government, liabilities about which taxpayers should be aware. The Government is urged to comply with the law promptly and to cease using blanket invocations of "national security" to justify violations of individual privacy.

V. <u>The Government's Proposed Guidance on the Retention and Acquisition of Internet Connection Records Threaten Privacy</u>.

61. Access to Internet Connection Records (ICRs) was controversial during the passage of the Investigatory Powers Act. The Government's new proposals reignite that

[42] Consultation Document, p. 19.

controversy with proposed changes to IPA Codes of Practice that threaten to undermine privacy by increasing in the intrusiveness of surveillance.

62. ICRs can reveal which newspapers we read online, where we shop online, what interest-based forums we join, and whether we access pornography. They reveal whether a person has visited the site for a charity that provides support for people with mental health problems or learning disabilities or HIV, or for people considering abortion.[43]

63. It is not difficult to imagine the chilling effect the ability to retain and access ICRs has on individuals' privacy and freedom of expression. Adolescents who might visit certain websites as they question their sexuality or gender identity; people with specific legal problems who might seek online legal guidance or advice from speciality law firms; people with medical conditions trying to make sense of their doctors' latest advice; people using dating websites (or websites for those wishing to conduct an affair); people expressing their political views on online forums; people gambling online; and people seeking to view legal pornography in the privacy of their own homes — all of these people must now consider, under the IPA, that the Government has (and exercises) the power to demand that their internet service provider keep, log, and on request share with Government a list of the websites and, potentially, the particular pages that they have visited.

64. Independent experts have questioned the rationale for retaining such data. The Independent Reviewer of Terrorism Legislation noted in June 2015 that the government failed to demonstrat that "access to weblogs is essential for a wide range of investigations" and stated that, even within the law enforcement community, "it is widely accepted" yet"the compulsory retention of web logs would be potentially intrusive."[44] He observed that no other European or Commonwealth country appears to compel the retention of such data, and that Canadian and American law

[43] Liberty fully briefed Parliament on its concerns about the retention and acquisition of ICRs during the debate over the IPA. Liberty's Briefing on 'Internet Connection Records' in the Investigatory Powers Bill for Report Stage in the House of Lords (October 2016) (available at https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%20briefing%20on%20ICRs%20for%20Report%20Stage%20in%20the%20House%20of%20Lords.pdf).

[44] David Anderson QC, Independent Reviewer of Terrorism Legislation: A Question of Trust: Report of the Investigatory Powers Review (June 2015) paragraphs 9.60–9.61. In paragraphs 9.53–9.54 of that report, Mr Anderson defines "web log" to "include websites visited up to the first '/' of its [URL], but not a detailed record of all web pages that a user has accessed".

enforcement represented "that there would be constitutional difficulties in such a proposal."[45] He concluded that while "retained records of user interaction with the internet (whether or not via web logs) would be useful … that is not enough on its own to justify the introduction of a new obligation on CSPs, particularly one which could be portrayed as potentially very intrusive on their customers' activities."[46]

65. Under section 21(6) of the Regulation of Investigatory Powers Act 2000,[47] communications data did not include anything beyond the domain name in an ICR. This was an important (if incomplete) limit on the intrusiveness of internet surveillance, in that it allowed the Government to learn, for example, that a person visited the New York Times web page, "www.nytimes.com", but not the specific page the New York Times has set up to receive information from confidential sources ("www.nytimes.com/newsgraphics/2016/news-tips/").

66. The Government's Autumn 2016 Draft Communications Data Code of Practice made clear that the underlined text in the example above (unless it contained usernames and authorisations or a port) were excluded from communications data.[48] However, the Government's new Draft Communications Data Code of Practice (dated November 2017 and released with the announcement of this consultation) does not contain this exclusion and makes clear that, at least in some circumstances, communications data may include a full web address.[49] This is possible under the IPA because there is no equivalent provision in the IPA to section 21(6) of RIPA.

---

[45] David Anderson QC, Independent Reviewer of Terrorism Legislation, A Question of Trust: Report of the Investigatory Powers Review (June 2015) paragraph. 9.55.

[46] David Anderson QC, Independent Reviewer of Terrorism Legislation, A Question of Trust: Report of the Investigatory Powers Review (June 2015) paragraph 14.33.

[47] Section 21(6) provided: "that expression ["communications data"] includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored".

[48] Home Office, *DRAFT Communications Data Code of Practice* (Autumn 2016) paras 2.54–2.55. Paragraph 2.55 stated: "With the exception of the port, and in certain circumstances the userinfo, these elements of a URL, where present, will not constitute communications data." "[T]hese elements" were explained in paragraph 2.54 included "path and optional parameters, which are analogous to a file path on a computer. In the example of socialmedia.com/profile/homethe /profile/home is the path" and "[t]he optional query parameters and fragments. These query parameters (identified by a '?' in the URL) contain data that doesn't fit within a hierarchical path structure and can locate certain content".

[49] Home Office, *Communications Data: Draft Code of Practice* (November 2017) paras 2.64–2.65.

67. This proposed change to the Codes of Practice is a significant change in a particularly controversial aspect of the IPA scheme and a threat to individual privacy. It is concerning that the Government does not mention this change in its consultation announcement or, apparently, seek public consultation on it. The Government should reconsider this change and institute appropriate safeguards for the retention and acquisition of ICRs.

VI. The Proposed Amendments Do Not Contain Adequate Safeguards for Privacy.

A. The Scheme for Independent Authorisation of Requests to Access Communications Data Should Be Stronger.

68. The Government accepts that the CJEU's judgment requires independent authorisation of requests to access communications data, acknowledging that the "CJEU's judgment is clear that requests to acquire retained communications data must be approved by a court or independent administrative body" and that the current IPA scheme does not satisfy this requirement.[50]

69. To address this problem, the Government proposes establishing a new Office for Communications Data Authorisations ("OCDA"), a non-judicial administrative body under the auspices of the Investigatory Powers Commissioner that shall authorise requests to access communications data.

70. Liberty has long called for judicial authorisation for all public authority requests to use investigatory powers. It is the proper constitutional function of the independent judiciary to act as a check on the use of intrusive powers by State bodies and to oversee the application of the law to individuals. Judges are professionally best equipped to apply the important legal tests of necessity and proportionality, to oversee the protection of individuals' rights, and to fairly probe public authorities' justifications for invoking such powers. We urge the Government to reconsider its proposal and subject all requests to robust review by the judiciary.

[50] Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017, p.18

71. At present, the IPA subjects most local authority applications to judicial approval by a magistrate. The Government's proposals would remove this requirement and would instead require administrative approval from OCDA. This proposed change is a step backwards in the privacy safeguards around local councils' requests to access individuals' private data.

72. Government should, at a minimum, create a requirement that OCDA refer to Judicial Commissioners any application of novelty, breadth or complexity, and any involving legally privileged or journalistic source information. The Government's proposal acknowledges that such applications require special consideration,[51] and require OCDA to seek guidance from a Judicial Commissioner in some cases,[52] but these provisions are too narrow and, even when they do apply, they allow the public authority to ignore the recommendation of the Judicial Commissioner. The Government should also require that officials of OCDA be made judicial officers and be required to take the judicial oath. They should be appointed on merit by the Judicial Appointments Commission, like judicial members of any other public tribunal.

73. The Government's proposals would permit internal authorisation by a designated senior officer in urgent cases. However, unlike the other urgent authorisation procedures in the IPA, the proposals do not provide for post-facto authorisation by an independent body. At a minimum, the Government should require that OCDA is notified of any urgent request and that OCDA consider that request retrospectively as promptly as possible, such that it may be revoked or limited if it is overbroad or otherwise inappropriate.

B. <u>The Proposed Amendments Ignore the Requirement for Notification of People Whose Data Has Been Accessed.</u>

74. The CJEU's judgment is unequivocal about the necessity of notifying individuals affected by access to retained data. It is clear that this is an important measure to ensure that safeguards are respected and to enable access to legal remedy.

[51] Home Office, *Communications Data: Draft Code of Practice* (November 2017) paras. 8.8-8.55.

[52] Home Office, *Communications Data: Draft Code of Practice* (November 2017) para. 8.52.

75. The CJEU outlined the requirement for independent authorisation of access requests in paragraph 120, "*in order to ensure, in practice, that those conditions* [the serious crime and individualised suspicion thresholds, inter alia] ***are fully respected",*** before addressing notification as an additional requirement in paragraph 121 (emphases added):

    "Likewise, the competent national authorities to whom access to the retained data has been granted ***must notify the persons affected****, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities.* ***That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy*** *(…)"*[53]

76. However, the Government resists respecting this element of the ruling. It considers that application to the Investigatory Powers Tribunal (IPT) provides access to redress which, it suggests, somehow negates the explicit requirement set out in the judgement that persons affected are notified after the fact.[54]

77. This is plainly incorrect. The requirement of notice and the requirement of a meaningful system for redress to people given notice are obviously two separate concepts. The presence of the latter cannot excuse the absence of the former. A system of redress has no (or virtually no) function if individuals are not aware of interference with their rights.

78. Moreover, the IPT recently constructed a new hurdle for applicants: those wishing to apply to the Tribunal now have to show that "*due to their personal situation, [they are] personally at risk of being subject to such [investigatory powers] measures*". In the *Human Rights Watch & Others* case, the Tribunal found that six NGO and individual claimants could demonstrate that they were at risk of being subject to such measures but that more than 600 private individuals could not.[55]

---

[53] Court of Justice of the European Union, Judgmentt of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 121

[54] Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017, p.20

[55] [2016] UKIPTrib15_165-CH available at - http://www.ipt-uk.com/docs/Human_Rights_Watch_FINAL_Judgment.pdf

79. Absent a notice requirement, people may never have any idea that their data has been swept up by investigatory powers measures. There is, for example, no way for a person to know that their location information has been subject to a retention notice served on their mobile service provider because they happened to be in a public area of interest to the security services, or for a person to know that their mobile phone traffic and location data was accessed as part of the deployment of a IMSI catcher (also known as a cell-site simulator) used in a law enforcement or intelligence operation.

80. Notification is indeed essential to enable a meaningful right to redress – but notification is required by the CJEU as a general and vital safeguard, *"to ensure, in practice, that those conditions* [safeguards] *are fully respected"*[56]*.* It is a measure that provides vital accountability and helps address the *"very far-reaching"* and *"particularly serious"* interferences with Articles 7 and 8 of the Charter as described in the CJEU's judgment:

"*The fact that the data is retained* ***without the subscriber or registered user being informed*** *is likely to* ***cause the persons concerned to feel that their private lives are the subject of constant surveillance****".*[57]

81. Similarly, the *Digital Rights Ireland* judgement in relation to Directive 2006/24, to which the *Watson* judgment applies, was clear on the importance of notification as a safeguard for fundamental rights (emphases added):

"It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, ***wide-ranging****, and it must be considered to be* ***particularly serious****. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the* ***fact that data are retained and subsequently used without the subscriber or registered user being informed*** *is likely to* ***generate in the minds of the persons***

[56] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 121

[57] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 100.

***concerned the feeling that their private lives are the subject of constant surveillance**."*[58]

82. Post-notification is an international standard for Government surveillance legislation. If a person's Article 8 and other HRA protected rights have been infringed, in order to have access to an effective remedy as required under human rights law, the person must first be made aware of a possible breach. This was stated by the ECtHR in *Klass v Germany* in 1978 and reiterated in *Weber and Saravia v Germany* in 2006 (emphasis added):

*"**The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards** against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively"* (see Klass and Others, cited above, pp. 26-27, § 57).[59]

83. In *Zakharov v Russia* the ECtHR found that judicial remedies for those subjected to interception in Russia were generally ineffective, particularly in light of the total absence of any notification requirement and thus no meaningful ability to challenge surveillance measures.

84. In *Szabo and Vissy v Hungary* the Court held:

*"As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, **information should be provided to the persons concerned**…In Hungarian law, however, no notification, of any kind, of the measures is foreseen. This fact, coupled with the absence of any formal remedies in case of abuse, indicates **the legislation falls short of securing adequate safeguards**."*[60]

[58] Court of Justice of the European Union, Judgment of 8.4.2014 – Joined Cases C-293/12 *Digital Rights Ireland Ltd.* and C-594/12 *Kärntner Landesregierung and Others* (ECLI:EU:C:2014:238): para. 37.

[59] *Weber and Saravia v Germany*, 2006, application 54934/2000, para. 135.

[60] Szabo and Vissy v Hungary, paragraph 86.

85. The IPA provides for a particularly opaque system whereby even error reporting obstructs individuals' right to redress. The IPA provides for the Investigatory Powers Commissioner to inform a person subjected to a surveillance error by a public authority (but not a CSP) only if it is "serious", which the Act defines as causing "significant prejudice or harm to the person concerned"[61] (terms which are left undefined). In the Act, the Government made the startling provision that a breach of a person's fundamental rights is *not* sufficient to constitute a serious error[62] – i.e. a breach of one's rights does not of itself constitute harm. Furthermore, the Act imposes a restriction that the IPC may not inform someone that their rights have been breached in a serious error *unless* this threshold of significant prejudice or harm is met.[63]

86. The serious error must meet an additional criterion of being a "relevant error", which is a furher arbitrary threshold to notification. The proposed new Draft Code of Conduct notes that the definition of "relevant error" has yet to be defined, and will be defined at the will of the Government in a forthcoming Code of Practice under Schedule 7 of the IPA.[64]

87. The restriction imposed by s. 231 (3), (7) and (9) may obstruct the IPC from informing a person that their Convention rights have been breached (unless an additional test is met), despite the fact that they are aware of the breach. As such, the IPC may be complicit in obstructing the affected person's right to redress. It is wholly inappropriate and unconstitutional to require that the IPC, of high judicial office, is forced to actively deny people their fundamental rights in this way. To describe this arrangement as being an effective substitute for the automatic right to notification required by the CJEU is wrong.

88. If a person is not informed that they have been subjected to investigatory powers, let alone informed that their rights have been breached, they will be denied the right to exercise their right to remedy and bring proceedings against the authority in breach,

[61] Investigatory Powers Act 2016, s.231(2)

[62] Investigatory Powers Act 2016, s.231(3)

[63] Investigatory Powers Act 2016, s.231(7)

[64] Home Office, *Communications Data: Draft Code of Practice* (November 2017) para. 24.23.

as provided for by s.7(1) of the HRA. The demonstration of 'harm', however defined, or indeed the demonstration of being at personal risk of investigatory powers, is irrelevant to this right.

89. The CJEU's judgment is clear that notification is *"in fact, necessary"* to safeguard rights and enable redress. It is not considered merely beneficial in addition to the function of the IPT, which the Court had the opportunity to consider before making its judgment, but necessary. As the Court acknowledged, it is of course important that operational concerns are considered when judging whether notification should be given in each case. However, such operational concerns should not trump the presumption that the right of innocent individuals to be notified that they have been subjected to the use of investigatory powers is to be upheld. Indeed, communications data is routinely used in criminal prosecutions every day. Anyone attending court will hear and see detailed use of communications data, including entity data and events data involving defendants, victims and witnesses. In particular, a Defendant already has full access to the communications data relied on by the prosecution and relevant to his or her defence. But there are no similar arrangements for innocent witnesses or victims, who will not be notified what data belonging to them was obtained and used, so that they can challenge the use if it was inappropriate.

C. <u>The Proposed Amendments Ignore the Requirement that Retained Data Be Held in the EU.</u>

90. The CJEU's judgment was clear that any scheme for retention of communications data "must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period."[65] This legally mandated safeguard is necessary to ensure that the data is retained within the jurisdiction of applicable privacy laws so that people's rights can be upheld.

91. The Government proposes to ignore this aspect of the CJEU's decision entirely, stating that notwithstanding the judgment, it "considers that it would not be appropriate to make further provision on security on the face of the legislation".[66]

---

[65] Court of Justice of the European Union, Judgment of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 122.

[66] Consultation Document, p. 17.

92. The Government had every opportunity when it argued before the CJEU to raise any logistical or logical objections to the requirement to retain data within the EU. Either it did not raise them or the court found them insufficient to outweigh important privacy rights. Either way, it is wholly inappropriate for the Government to choose to ignore this court judgment, let alone to seek public approval for its apparent disregard for the rule of law.

93. Notably, we agree with the Government that the CJEU's judgment does not seek to restrict transfers of data where the requirements of EU law (including Article 8) are met. The requirement to hold retained data in the EU simply ensures that those privacy laws apply.

VII. The Government's Erroneous Legal Argument About the Application of the CJEU's Judgment to Business Data Highlights the Inappropriate Aspects of this Consultation.

94. In its proposal, the Government offers a legal opinion that "none of the requirements of the CJEU's judgment relate to the acquisition of data that is being held for business purposes, rather than pursuant to a retention obligation imposed by Government."[67] Although it is true that the judgment does not refer to data held for business purposes, there is no basis for concluding that data held for business purposes and which is then subject to a retention notice is therefore excluded from the judgment. If this is what the Government means to suggest, then there is no basis for such an interpretation of the CJEU's judgment.

95. The Government's decision to include this point in the consultation, however, is even more mystifying than its legal reasoning. Despite drawing a distinction as a matter of law between data held for business purposes and data held pursuant to a retention obligation, the Government does not propose any policy based on that purported distinction. Without a policy on which to consult, there is no valid reason to address this point in the public consultation process. The Government should not attempt to use the public consultation process to legitimise efforts to undermine the force of court rulings constraining Government power.

[67] Consultation Document, p. 12.