Casting the Dragnet: Communications Data Retention Under the Investigatory Powers Act

Public Law

2018

Casting the dragnet: communications data retention under the Investigatory Powers Act

Jennifer Cobbe

Subject: Information technology . **Other related subjects:** European Union. Human rights.

Keywords: Communications data; Data protection; Data retention; EU law; Fundamental rights; Investigatory powers; Personal data; Privacy; Proportionality

Legislation:

Investigatory Powers Act 2016 (c.25) Pt 3, Pt 4

Directive 2002/58 art.15

Charter of Fundamental Rights of the European Union art.7, art.8, art.52

Cases:

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127 (ECJ (Grand Chamber))

Tele2 Sverige AB v Post- och telestyrelsen (C-203/15) EU:C:2016:970; [2017] Q.B. 771 (ECJ (Grand Chamber))

P.L. 10 In November 2016 the Investigatory Powers Act received Royal Assent. The 2016 Act was hailed by the Government as bringing the UK's surveillance framework into the twenty first century and better allowing security and intelligence agencies to combat terrorism and serious crime. The Investigatory Powers Act raises a range of concerns, with its progress through Parliament marked by sustained opposition ***P.L. 11*** from civil liberties groups. One of the most controversial aspects of the 2016 Act is the bulk communications data retention and disclosure framework in Pts 3 and 4. This article concerns the compatibility of that framework with EU law in light of CJEU decisions in *Digital Rights Ireland* [1] and *Watson*.[2] It will begin by briefly providing some background, will then broadly set out the requirements that can be determined from these decisions, and will proceed to take a more detailed analysis of these requirements in relation to Pts 3 and 4.

Communications data retention prior to the 2016 Act

Between 2009 and 2014, internet service providers ("ISPs") served notice by the Home Secretary[3] were required to store some communications data for 12 months[4] under the Data Retention (EC Directive) Regulations 2009, pursuant to the Data Retention Directive.[5] This involved retaining metadata,[6] which is the "who", "when", "where", and "for how long" of data, rather than the content of communications (a common analogy is that metadata is the envelope rather than the letter, which is content). In 2014 the CJEU found in *Digital Rights Ireland* that the Data Retention Directive was incompatible with arts 7 (respect for private and family life, including privacy of communications)[7] and 8 (protection of personal data)[8] of the EU's Charter of Fundamental Rights.[9] As a result the Data Retention and Investigatory Powers Act [10] was quickly passed in order to pre-empt challenges to the 2009 Regulations based on *Digital Rights Ireland*. The High Court subsequently followed *Digital Rights Ireland* to find that s.1 of the 2014 Act was incompatible with the Charter and the Government was given until April 2016 before it would be disapplied.[11] The Court of Appeal indicated that it was minded to disagree with the High Court but referred to the CJEU for a preliminary ruling for clarification.[12] In December 2016 the CJEU in *Watson* confirmed the incompatibility of 2014 Act -style retention. In any case, the 2014 Act was subject to a sunset clause meaning that it would be automatically repealed on 31 December 2016.[13] This was the impetus behind the 2016 Act. ***P.L. 12***

Digital Rights Ireland and Watson

Digital Rights Ireland and *Watson* together provide the requirements in EU law to which the 2016 Act must conform both in terms of the retention of communications data and in terms of access to

retained data.

Digital Rights Ireland considered the validity of the Data Retention Directive in relation to arts 7 and 8 of the Charter read alongside art.52(1), which states that for interferences with Charter rights to be potentially justifiable they must respect the essence of those rights.[14] The CJEU held that legislation permitting the retention only of metadata and requiring measures be adopted to protect the security and integrity of retained data does not adversely affect the essence of arts 7 and 8, respectively, and so constitutes a potentially justifiable interference with those rights.[15] According to *Digital Rights Ireland*, retention may be justified provided it satisfies an objective of general interest[16] (such as, but not necessarily limited to, fighting serious crime or terrorism),[17] and is limited to what is strictly necessary to pursue the objective.[18] Access to retained data for the purpose of fighting crime should be limited only to offences determined by objective criteria to be sufficiently serious to justify the interference with arts 7 and 8.[19] Access should also be subject to prior review by a court or independent administrative body.[20]

Watson addressed the question of the compliance of bulk data retention with the ePrivacy Directive [21] read alongside arts 7, 8, and 52(1) of the Charter [22]. In doing so the CJEU drew the purposes for which data may be retained narrower than in *Digital Rights Ireland* to include only national security, defence, public security,[23] and serious crime.[24] The court also went much further than *Digital Rights Ireland* in finding that in order to be proportionate retention must be an exception rather than the rule, [25] as well as being limited to what is strictly necessary for the purpose being sought.[26] *Watson* also addressed the question of requirements for access to retained data.[27] The court found that the purposes for which retained data can be accessed must genuinely and strictly correspond to the same purposes for which ***P.L. 13*** it can be retained.[28] In order to be proportionate, access to retained data must be limited to what is strictly necessary.[29] In order to ensure that this is the case, access must normally be subject to prior review by a court or an independent administrative body.[30] Further, persons whose data has been accessed should be notified as soon as doing so would not jeopardise an investigation.[31]

Seven requirements can broadly be distilled from *Digital Rights Ireland* and *Watson* that the 2016 Act must satisfy. The first four relate to retention under Pt 4. These are that retained data must exclude content, that ISPs must be required to ensure the security and integrity of retained data, that the purpose being sought by retention can only extend to national security, defence, public security, and fighting serious crime, and that retention must be proportionate with data retained as an exception rather than as the rule and only to the extent strictly necessary for the purpose being sought. The final three relate to obtaining data under Pt 3. These are that access to data must be only for a purpose genuinely and strictly corresponding to those for which it can be retained, that in order to be proportionate data can be accessed only to the extent strictly necessary, and that there are required safeguards and oversight mechanisms.

Communications data retention under the 2016 Act

Part 4 of the 2016 Act provides for the bulk retention of communications data. Internet service providers who have been served a retention notice are required to retain all relevant communications data covered by the retention notice sent from devices connected to their network for a maximum of 12 months.[32]

The nature of retained data

Digital Rights Ireland established that legislation permitting the acquisition of knowledge of the content of a communication would be contrary to the essence of art.7 of the Charter and thus unjustifiable.[33] Retention must therefore not include the content of communications in order to be a potentially justifiable interference with art.7.

The data that ISPs may be required to retain under the 2016 Act is "relevant communications data".[34] This is defined as a subset of communications data that identifies the sender or recipient of a communication; the time or duration of a communication; the type, method, pattern, or fact of communication; the system from, to, or through which a communication is transmitted; or the location of any such system.[35] Communications data includes certain types of entity data and events ***P.L. 14*** data, on one hand, and explicitly excludes the content of communications, on the other.[36] As communications data excludes content, the first step in determining whether retention is in fact contrary to the essence of art.7 is to look at how the 2016 Act defines content.

Under the 2016 Act content in this context is any element of a communication, or data attached to or associated with a communication, which reveals anything that might reasonably be considered to be the meaning of that communication.[37] This does not include any meaning arising from the mere fact of the communication having occurred or from data relating to the transmission of the communication. This may be compared with the definition of relevant communications data under the 2014 Act, which excludes data revealing the content of a communication,[38] rather than the meaning. It seems that in replacing the 2014 Act Parliament has chosen not to carry over a definition that excludes content generally from communications data, instead providing one that excludes only the meaning of a communication. However, it is not clear precisely what the "meaning" of a communication extends to. It is also not clear that data revealing the meaning of a communication is the same as data providing knowledge of its content. It is quite conceivable that there could be elements of a communication that provide knowledge of its content, and so would be impermissible to retain per *Digital Rights Ireland*, but do not reveal its *meaning* and so would not be considered to be content for the purposes of the 2016 Act. This could be, for example, a telephone number conveyed in the body of an email (i.e. providing knowledge of some of the content), but not text surrounding it that relates to it and provides context (i.e. revealing the meaning of the email).

It is not clear that all data providing knowledge of the content of a communication is explicitly not communications data. So it is necessary to look at what is explicitly included in order to determine whether or not retention under the 2016 Act interferes with the essence of art.7 of the Charter. Entity data is that which is about an entity (a person or a thing)[39] or an association between an entity and a telecommunication system (a system for transmitting communications electronically)[40] or telecommunications service (a service providing access to or use of a telecommunication system)[41] and which identifies or describes the entity.[42] Events data is that which describes an event on, in, or by means of a telecommunication system and consisting of one or more entities engaging in a specific activity at a specific time.[43] The kinds of entity data or events data that may be considered to be communications data include, inter alia, data held by an ISP about a customer and relating to a service provided to them, data included as part of a communication for the purposes of the system by which it is being communicated, and data which is held by an ISP about the architecture of a telecommunication system and is not about a specific person.[44] In this a telephone ***P.L. 15*** number in the body of an email would not be events data or entity data and so, while perhaps not content for the purposes of the 2016 Act, it would not be considered to be communications data and could not be retained. Communications data therefore appears to include only metadata—relating to the functioning of telecommunication systems, the provision of telecommunications services, and the transmission of communications—rather than data which would provide knowledge of the content of a communication. As relevant communications data is a subset of communications data, it is also limited to metadata. Retention of metadata is not contrary to the essence of art.7 and is therefore capable of being justified provided it is for permitted purposes and is proportionate to those purposes.

The security of retained data

Digital Rights Ireland held that legislation providing for bulk data retention must set out rules for protecting the data retained by ISPs. These must require a high level of protection and security be applied to the data and require the data to be irreversibly destroyed at the end of the retention period.[45] They should also require retained data to be kept within the EU, and compliance must be subject to review by an independent authority as per art.8 of the Charter.[46] *Watson* restated these four requirements.[47]

The 2016 Act requires that ISPs must destroy data once its retention is no longer authorised under Pt 4, provided its retention isn't otherwise authorised by law.[48] Destruction may take place at monthly or shorter intervals as appear to the ISP to be reasonably practicable.[49] The Information Commissioner must review ISPs' compliance with requirements under Pt 4 relating to the integrity, security, or destruction of retained data.[50] To that extent the 2016 Act meets the requirements of *Digital Rights Ireland* and *Watson*. However, in terms of the level of protection applied to retained data and the requirement data be kept in the EU, the 2016 Act is not in compliance.

Section 92 of the 2016 Act covers the integrity and security of data retained by ISPs. Retained data is required to be "of the same integrity, and subject to at least the same security and protection"[51] as data on the system from which it is derived. The storage and processing of that data is regulated by the Privacy and Electronic Communications (EC Directive) Regulations 2003.[52] Regulation 5 thereof requires that ISPs take "appropriate"[53] technical and organisational measures, which must at least ensure that data can be accessed only by authorised personnel (a requirement repeated in the 2016

Act)[54] for legally authorised purposes.[55] It also requires that ***P.L. 16*** data must be protected against "accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure"[56] (again a requirement repeated in the 2016 Act).[57] Regulation 5(4) defines "appropriate" in this context. A measure is appropriate where, taking into account the state of technological developments and the cost of implementation, it is proportionate to the risks being safeguarded against.[58] However, *Digital Rights Ireland* requires that when securing retained data ISPs are to ensure a particularly high level of protection and security without regard to economic considerations.[59] As such, the requirement that ISPs secure retained data with the same security and protection as data on the system from which it is derived does not meet the standard set by the CJEU. Further, the 2016 Act does not require that data retained by ISPs be kept within the EU. The Data Protection Act 1998 places restrictions on the transfer of personal data to countries outside the EEA,[60] which would include relevant communications data insofar as it permits the individual to whom the data relates to be identified.[61] But *Watson* says that the legislation permitting retention must itself provide for retained data to be kept within the EU.[62] This means that relying on other legislation, such as the Data Protection Act, is not permissible.

As the 2016 Act fails to meet these requirements, the storage of retained data by ISPs provided for by the Act constitutes an unjustifiable interference with art.8 of the Charter.

Purposes for which data may be retained

Watson held that data retention is only permissible for a limited number of purposes as permitted by the ePrivacy Directive read in conjunction with arts 7 and 8 of the Charter. Article 5(1) of the ePrivacy Directive says that as a general rule a user's data may not be stored by another person without the consent of that user.[63] This is subject to exceptions permitted by art.15(1) of that directive (explicitly including data retention) for various purpose including to safeguard national security, defence, and public security, and for fighting crime.[64] Acknowledging that the interference with arts 7 and 8 of the Charter posed by bulk data retention is "very far-reaching and … particularly serious",[65] *Watson* held that in terms of fighting crime only the purpose of fighting *serious* crime is a permissible exception.[66]

Section 87(1) of the 2016 Act provides that retention notices may require an ISP to retain relevant communications data for one of the purposes set out in ***P.L. 17*** s.61(7).[67] While these purposes include national security and fighting crime,[68] this is not limited only to serious crime. Further, s.61(7) sets out a variety of other purposes including, among others, protecting public health, assessing or collecting any taxes or duties payable to government departments, preventing death or injury, assisting investigations into alleged miscarriages of justice, assisting in identifying someone who is deceased or otherwise unable to identify themselves, and the regulation of financial services markets.[69] Accordingly, the purposes for which data can be required to be retained under the 2016 Act go beyond those which are permitted by *Watson*.

Proportionality of data retention

The principle of proportionality requires that limitations on arts 7 and 8 of the Charter are permitted only so far as they are strictly necessary.[70] As such, *Digital Rights Ireland* and *Watson* both set out requirements that must be met in order for a retention regime to be strictly necessary and thus proportionate.

Digital Rights Ireland requires that retention legislation provides clear and precise rules governing the scope and application of interferences with Charter rights,[71] and established two grounds for determining the strict necessity of data retention. The first is that retention cannot cover all persons, all means of electronic communication, and all communications data without any differentiation, limitation or exception and cannot cover people for whom there is no evidence capable of suggesting that they have a link, even indirectly or remotely, with serious crime.[72] Additionally, retention must include safeguards for data subject to professional confidentiality, and must require a relationship between the data being retained and a threat to public security.[73] In particular, the latter means that retention should be limited to a particular time period, geographical location, or circle of people likely to be involved in serious crime, or to people for whom the retention of their data could contribute to fighting serious crime. The second ground is that the period of time for which data is to be retained should distinguish between types of data based on their possible usefulness.[74] The length of the retention period should be based on objective criteria to ensure that it is limited to what is strictly necessary.[75]

Watson found that "general and indiscriminate retention"[76] as the rule rather than the exception,[77] covering all users without differentiation, limitation, or ***P.L. 18*** exception according to the objective pursued,[78] and not requiring any particular relationship between the data to be retained and the purpose of retention,[79] "exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society".[80] The requirement that retention must be an exception rather than the rule goes beyond the limits established in *Digital Rights Ireland*, which permitted such bulk retention provided the required limitations and exceptions were clearly set out. *Watson* says that legislation must place retention itself as an exception to the general rule set out in art5 of the ePrivacy Directive. As such, and while the judgment says that *targeted* retention is permissible provided it is limited to what is strictly necessary,[81] the result of *Watson* is that bulk data retention can never be considered to be strictly necessary and thus can never be proportionate.

The 2016 Act fails to meet the proportionality requirements of either *Digital Rights Ireland* or *Watson*. Retention notices may be tailored to an extent, including by requiring that only data which meets a certain description[82] or is from a certain time period[83] is retained. But s.87 does allow for ISPs to be required to retain "all data"[84] indiscriminately, without differentiation, limitation, or exception, and without clear safeguards for data subject to professional confidentiality. Further, s.87 does not require any relationship between data to be retained and the purpose being pursued or any link between that data and a threat to public security. Nor does it require the retention period, while limited to a maximum of 12 months,[85] to be determined based on objective criteria and limited to what is strictly necessary. Finally, s.87 does not set out clear and precise rules on the scope and application of retention. Instead the Secretary of State can issue notices containing "other requirements, or restrictions, in relation to the retention of data"[86] and making "different provision for different purposes".[87] As such, s.87 does not provide only for retention that is justified as a strictly necessary and therefore proportionate interference with arts 7 and 8 of the Charter as per *Digital Rights Ireland*. Perhaps most significantly, the 2016 Act allows for bulk retention as the rule rather than the exception, exceeding the limits of what can be considered strictly necessary, and so cannot be proportionate as per *Watson*. ***P.L. 19***

Access to communications data

Part 3 of the 2016 Act provides for the disclosure of communications data to relevant public authorities upon request.[88] Relevant public authorities include those public authorities listed in Sch.4[89] as well as local authorities.[90]

Purposes for which data may be obtained

Watson determined that the purposes for which communications data may be accessed must "genuinely and strictly"[91] correspond to one of those established by art.15(1) of the ePrivacy Directive read alongside arts 7 and 8 of the Charter, namely national security, defence, public security, and fighting serious crime.

Digital Rights Ireland requires that "serious crime" be defined by objective criteria.[92] In the 2016 Act this is defined as offences where an individual with no previous convictions could reasonably be expected to be imprisoned for three years or more, or those that involve violence, result in substantial financial gain, or involve a large number of people acting together for a common purpose,[93] satisfying *Digital Rights Ireland* 's requirement.

However, communications data can be obtained in the pursuit of several purposes beyond those permitted by *Watson*. These include, among others, for protecting public health, for assessing or collecting any taxes or duties payable to government departments, for preventing death or injury, and for assisting investigations into alleged miscarriages of justice.[94] This does not satisfy the requirement in *Watson* limiting the purposes for which communications data can be obtained.

Proportionality of disclosure

As with retention, *Watson* holds that access to data must not exceed the limits of what is strictly necessary in order to be proportionate.[95] In particular, this means that legislation must provide clear and precise rules indicating in what circumstances and under which conditions data may be obtained for permitted purposes.[96] Legislation must provide that access normally be granted only to the data of individuals suspected of serious criminality (those suspected of planning, committing, having

committed, or being implicated in a serious crime).[97]

In terms of the circumstances in which communications data can be accessed under the 2016 Act, this can only be for use in a specific investigation or operation.[98] Some communications data takes the form of internet connection records ("ICRs"). ***P.L. 20*** These are defined in s.62(7) as the subset of communications data generated or processed by an ISP in the process of supplying an internet connection to a customer that identifies, or assists in identifying, the online service that is being used via that connection (which could be a particular website, email service, messaging service, etc.).[99] Disclosure of communications data other than ICRs is not limited only to that concerning individuals suspected of any criminality, let alone serious criminality.

Several conditions apply to obtaining ICRs that do not apply to obtaining other communications data. Local authorities may not obtain ICRs in order to access data that can only be obtained through ICRs.[100] For public authorities that are not local authorities, ICRs may only be disclosed where one of three conditions is met.[101] The first is that it is necessary to identify unknown persons or devices using a known internet service, but this is not limited to individuals suspected of serious criminality.[102] The second relates to obtaining data for purposes other than fighting crime[103]. The third, which does relate to the purpose of fighting crime, is that obtaining an ICR is necessary either to determine which service is being used, when it is being used, and how it is being used by a person or device whose identity is known, or to determine where or when a known person or device is accessing or running software which involves making available or acquiring material whose possession is a crime.[104] However, this third condition is not limited only to the purpose of fighting *serious* crime, but also to "other relevant crime".[105] As such, ICR disclosure is also not limited only to those of individuals who are suspected of serious criminality, and is therefore not limited only to what is strictly necessary.

The communications data disclosure framework established by the 2016 Act does not therefore provide for a proportionate interference with fundamental rights.

Safeguards and oversight

Both *Digital Rights Ireland* and *Watson* require that requests for access normally be subject to prior review by a court or an independent administrative body.[106] This is to ensure that access to communications data is limited to what is strictly necessary. *Watson* further required that persons whose data has been accessed be notified once it is possible to do so without jeopardising an investigation.[107] The 2016 Act does not provide for individuals whose data has been disclosed to be notified.

Requests from local authorities for disclosure of communications data require the approval of a judge,[108] and so meet the required standard. But requests for data from public authorities other than local authorities can normally be authorised by ***P.L. 21*** senior officers within the requesting authority without requiring approval by a judge[109] (although the approval of a judicial commissioner is required for authorisations that would identify a journalistic source).[110] Senior officers may not normally grant authorisations for investigations they are working on,[111] and there are certain procedural requirements.[112] And before a senior officer within a relevant public authority can approve a request they must normally consult a single point of contact ("SPoC"), an individual within the authority responsible for advising others internally on requests.[113] Single points of contact advise on issues including the lawfulness of proposed authorisations, whether it is reasonably practicable to obtain the data sought, and any cost implications of a request.[114]

In order to determine whether in terms of public authorities other than local authorities the approval regime satisfies the requirements of *Watson* it is necessary at this point to attempt to determine what the CJEU may mean by "independent" in this context. The CJEU has previously discussed this[115] in relation to the requirement for independent oversight of compliance with the Data Protection Directive.[116] In that instance the court concluded that "independent" normally means "a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure".[117] In its view supervisory authorities "must act objectively and impartially. For that purpose, they must remain free from any external influence".[118] The CJEU went on to say that this

"precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task".[119]

Independence in the context of supervision of data protection, relevant to both the ePrivacy Directive

and to art.8 of the Charter and thus to access to retained data under the 2016 Act, appears to require both objectivity and impartiality, and, to that end, freedom from any external influence. The *Communications Data Draft Code of Practice* says that SPoCs provide "objective judgement",[120] but the code does not require SPoCs to act impartially. The code also states that senior officers shall take account of the SPoC's advice in assessing the necessity of an authorisation.[121] Single points of contact do not, however, have the power to block requests and are themselves permitted to authorise requests if they are also senior officers.[122] As such, it seems that in relation to public authorities other than local ***P.L. 22*** authorities the framework is not compatible with the requirements established in *Digital Rights Ireland* and *Watson* that access to communications data be subject to independent prior review.

Part 3 of the 2016 Act therefore does not provide the safeguards required to ensure that access to communications data is limited to what is strictly necessary and therefore proportionate to the purpose being sought.

Conclusion

There are serious issues with the communications data retention and disclosure framework under the 2016 Act. While retention does appear to be limited to metadata, Pts 3 and 4 of the 2016 Act do not meet other requirements established by the CJEU. The 2016 Act does not require a particularly high level of protection be applied to retained data or that it be kept in the EU. Retention notices can be issued in pursuit of a range of purposes other than those permitted. Retention is indiscriminate and is the rule rather than the exception. The length of the retention period is not objectively determined and limited to what is strictly necessary. The 2016 Act does not provide clear and precise rules governing the scope and application of retention. Communications data can be accessed for a variety of purposes other than those permitted. Access is not limited to data of individuals suspected of serious criminality. Finally, the oversight regime does not provide for independent prior review or for individuals whose data has been accessed to be notified when appropriate. Parts 3 and 4 of the 2016 Act are therefore an unjustifiable interference with art.15(1) of the ePrivacy Directive read alongside arts 7 and 8 of the Charter.

Jennifer Cobbe

Doctoral Candidate

Queen's University, Belfast

P.L. 2018, Jan, 10-22

---

1. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127*.

2. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289*.

3. Data Retention (EC Directive) Regulations 2009 (SI 2009/859) (the 2009 Regulations) reg.10.

4. 2009 Regulations regs 4, 5.

5. Directive 2006/24 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 [2006] OJ L105/54 (the Data Retention Directive).

6. 2009 Regulations reg.2; Sch.1 Pt 3.

7. Charter of Fundamental Rights of the European Union [2012] OJ C326/391 (Charter of Fundamental Rights) art.7

8. Charter of Fundamental Rights art.7.

9. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127*.

10. Data Retention and Investigatory Powers Act 2014 (the 2014 Act).

11. *R. (on the application of Davis) v Secretary of State for the Home Department [2015] EWHC 2092 (Admin); [2016] 1 C.M.L.R. 13*.

12. *R. (on the application of Davis) v Secretary of State for the Home Department [2015] EWCA Civ 1185; [2016] 1 C.M.L.R. 48*.

13. 2014 Act s.8(3).

14. Charter of Fundamental Rights art.52(1).

15. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [39]–[40].

16. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [38].

17. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [42].

18. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [46], [52].

19. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [60].

20. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [62].

21. Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37 (ePrivacy Directive).

22. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [62].

23. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [90].

24. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [102].

25. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [104].

26. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [96].

27. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [114].

28. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [115].

29. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [116].

30. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [120].

31. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [121].

32. Investigatory Powers Act 2016 (the 2016 Act) s.87.

33. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [39].

34. 2016 Act s.87(1).

35. 2016 Act s.87(11).

36. 2016 Act s.261(5).

37. 2016 Act s.261(6).

38. 2014 Act s.2(2).

39. 2016 Act s.261(7).

40. 2016 Act s.261(13).

41. 2016 Act s.261(11)

42. 2016 Act s.261(3).

43. 2016 Act s.261(4).

44. 2016 Act s.261(5).

45. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [67].

46. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [68].

47. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [122]–[123].

48. 2016 Act s.92(2).

49. 2016 Act s.92(3).

50. 2016 Act s.244.

51. 2016 Act s.92(1)(a).

52. Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) (the 2003 Regulations).

53. 2003 Regulations reg.5(1).

54. 2016 Act s.92(1)(b).

55. 2003 Regulations reg.5(1A)(a).

56. 2003 Regulations reg.5(1A)(b).

57. 2016 Act s.92(1)(c).

58. 2003 Regulations reg.5(4).

59. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [67].

60. Data Protection Act 1998 Sch.1 para.8.

61. Data Protection Act 1998 s.1(1).

62. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [122].

63. ePrivacy Directive art.5(1).

64. ePrivacy Directive art.15(1).

65. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [100].

66. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [102].

67. 2016 Act s.87(1).

68. 2016 Act s.61(7)(a) –(b).

69. 2016 Act s.61(7)(c) –(j).

70. *Tietosuojavaltuutettu v Satakunnan Markkinaporssi Oy (C-73/07) EU:C:2008:727; [2010] All E.R. (EC) 213* at [56]; *Volker und Markus Schecke GbR v Land Hessen (C-92/09) EU:C:2010:662; [2012] All E.R. (EC) 127* at [77].

71. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [54].

72. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [57]–[58].

73. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [58]–[59].

74. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [63].

75. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [64].

76. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [97].

77. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [104].

78. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [105].

79. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [106].

80. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [107].

81. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [109]–[111].

82. 2016 Act s.87(2)(b).

83. 2016 Act s.87(2)(c).

84. 2016 Act s.87(2)(b).

85. 2016 Act s.87(3).

86. 2016 Act s.87(2)(d).

87. 2016 Act s.87(2)(e).

88. 2016 Act Pt.3.

89. 2016 Act s.70.

90. 2016 Act s.73.

91. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [115].

92. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [46], [52].

93. 2016 Act s.263(1).

94. 2016 Act s.61(7).

95. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [116].

96. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [117].

97. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [119].

98. 2016 Act s.61(1).

99. 2016 Act s.62(7).

100. 2016 Act s.62(1).

101. 2016 Act s.62(2).

102. 2016 Act s.62(3).

103. 2016 Act s.62(4).

104. 2016 Act s.62(5).

105. 2016 Act s.62(6).

106. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238; [2015] Q.B. 127* at [62]; *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [120].

107. *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson (C-203/15); (C-698/15) EU:C:2016:970; [2017] 2 W.L.R. 1289* at [121].

108. 2016 Act s.75.

109. 2016 Act ss.61 –66.

110. 2016 Act s.77.

111. 2016 Act s.63.

112. 2016 Act s.64.

113. 2016 Act s.76.

114. 2016 Act s.76(5) –(6).

115. *European Commission v Germany (C-518/07) EU:C:2010:125; [2010] 3 C.M.L.R. 3*.

116. Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

117. *European Commission v Germany (C-518/07) EU:C:2010:125; [2010] 3 C.M.L.R. 3* at [18].

118. *European Commission v Germany (C-518/07) EU:C:2010:125; [2010] 3 C.M.L.R. 3* at [25].

119. *European Commission v Germany (C-518/07) EU:C:2010:125; [2010] 3 C.M.L.R. 3* at [30].

120. *Home Office, Communications Data Draft Code of Practice (TSO, 2016), para.4.33*.

121. *Home Office, Communications Data Draft Code of Practice, para.4.19*.

122. 2016 Act s.76(8).