THE PRESIDENT AND MEMBERS OF THE COURT OF JUSTICE OF THE EUROPEAN UNION

In **Case C-140/20**

G.D.

Plaintiff/Respondent

-and-

THE COMMISSIONER OF AN GARDA SÍOCHÁNA, THE MINISTER FOR COMMUNICATIONS, ENERGY AND NATURAL RESOURCES, IRELAND AND THE ATTORNEY GENERAL

Defendants/Appellants

WRITTEN OBSERVATIONS OF THE DEFENDANTS

The Defendants, represented by Maria Browne, Chief State Solicitor, Osmond House, Little Ship Street, Dublin 8, acting as Agent, accepting service by e-Curia with an address at the Embassy of Ireland, 28 route d'Arlon, Luxembourg, and assisted by Paul Gallagher SC, Attorney General of Ireland, Sean Guerin SC, David Fennelly BL and Lucy Dwyer BL, of the Bar of Ireland, have the honour to submit written observations in this reference for preliminary ruling from the Supreme Court of Ireland dated 25 March 2020.

Dated 7 August 2020

I. Introduction

1. By Order for Reference dated 25 March 2020, the Supreme Court of Ireland has referred six questions for preliminary ruling pursuant to Article 267 of the Treaty on the Functioning of the European Union.

2. This Reference follows in a long line of references from Member States' courts concerning the compatibility of national data retention legislation with EU law[1] in the wake of this Court's judgment in *Digital Rights Ireland & Others*.[2] Following the striking down of Directive 2006/24/EC ('the Data Retention Directive') in that judgment, the sole provision of EU law which in any way addressed data retention was Article 15(1) of Directive 2002/58/EC ('the e-Privacy Directive'). It is by reference to this provision that the Court has since assessed the compatibility of national data retention regimes with EU law. However, Article 15(1) does not, and was never intended to, provide a detailed framework for the regulation of data retention at EU level.

3. In the absence of any detailed legislative framework at EU level, this Court has taken on the task of defining the criteria by which national data retention regimes are to be assessed for their compatibility with EU law. In its judgment in *Tele2 Sverige/Watson*, the Court concluded that, while EU law did not preclude a Member State from adopting legislation permitting, as a preventive measure, "*the targeted retention of traffic and location data*",[3] Article 15(1) of the e-Privacy Directive, read in light of Articles 7, 8 and 11 of the Charter, precluded national legislation providing for what the Court described as "*the general and indiscriminate retention of all traffic and location data*".[4] The Court reached this conclusion without referring to any evidence on the form or feasibility of these different models of data retention. The references which have followed *Tele2 Sverige/Watson* illustrate the significant challenges that this judgment poses for the fight against crime and the safeguarding of national security across all Member States. They also underline why complex issues of this kind should not be determined in an evidential vacuum.

4. As a result, despite the many references which have followed *Digital Rights Ireland*, there remains very significant uncertainty about the circumstances in which data retention is permissible under EU law.

5. In contrast to the preceding references, in this Reference, the Supreme Court of Ireland has made critically important findings of fact, based on expert evidence adduced before the national court, on the form, feasibility and proportionality of data retention for law

---

[1] C-203/15, *Tele2 Sverige*; C-698/15, *Watson*; C-475/16, *K* (withdrawn); C-207/16, *Ministerio Fiscal*; C-623/17, *Privacy International*; C-511/18, *Quadrature du Net & Others*; C-512/18, *French Data Network & Others*; C-520/18, *Ordre des barreaux francophones et germanophone*; C-746/18, *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)*; C-793/19, *SpaceNet AG*; C-794/19, *Telekom Deutschland GmbH*.

[2] Judgment of 8 April 2014, *Digital Rights Ireland & Others*, C-293/12 and C-594/12, EU:C:2014:238.

[3] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 108.

[4] *Tele2 Sverige/Watson*, EU:C:2016:970, paragraph 112.

enforcement purposes. This Court is now presented with an opportunity to address the issue of data retention on a firm evidential foundation.

6. It is clear from this evidence that data retention is only effective as a law enforcement tool if it is general in scope at the retention stage. If, notwithstanding this evidence, the Court were to conclude that a general data retention regime is not permissible as a matter of EU law, this would be tantamount to prohibiting the use of data retention as a law enforcement tool despite its vitally important and increasingly relevant role in the fight against serious crime and threats to national security.

7. For this reason, the Court's judgment on this Reference will have far-reaching implications: first and foremost for the specific proceedings which have given rise to the Reference as well as for the very many other cases in which retained telecommunications metadata have been relied upon by the law enforcement authorities over the past decade in Ireland; and secondly, and more broadly, for the essential activities of law enforcement and security authorities and for the safety and protection of EU citizens across all Member States into the future.

II. The Factual and Legal Background to the Reference

8. The Supreme Court has summarised the essential features of the Irish legislative scheme in Appendix I and the facts of the specific case which has given rise to the Reference in Appendix II.[5]

9. This Reference is not a general and abstract challenge to the Irish data retention legislation. It arises in the context of criminal proceedings in which the Plaintiff, G.D., was tried and convicted of the murder of a vulnerable adult, E.O'H. Telecommunications metadata retained under Irish law played a highly significant role in identifying the Plaintiff as a suspect in the investigation of this crime and thereafter, alongside a significant body of other evidence, in the prosecution and conviction of the Plaintiff. In the course of the criminal proceedings, the trial judge rejected the Plaintiff's challenge to the admissibility of the evidence, which was based on this Court's judgment in *Digital Rights Ireland*. In advance of prosecuting his criminal appeal, the Plaintiff has brought these proceedings, challenging the validity of the Irish data retention legislation, the Communications (Retention of Data) Act 2011 ("**the 2011 Act**"), with a view to raising this issue on appeal.

10. The 2011 Act served to give effect to Directive 2006/24/EC in Irish law. Following the adoption of the Data Retention Directive, Ireland had challenged the legal basis on which the Directive had been adopted by way of action for annulment. In its judgment of 10 February 2009, this Court upheld the validity of the Data Retention Directive.[6] In subsequent infringement proceedings, the Court of Justice concluded that Ireland had failed to fulfil its obligations under the Data Retention Directive by failing to adopt

[5] Judgment of Mr Justice Clarke, Chief Justice ('Supreme Court Judgment'), paragraphs 3.1-3.3.

[6] Judgment of 10 February 2009, *Ireland v Parliament and Council*, C-301/06, EU:C:2009:68. That challenge was concerned with the legal basis on which the Directive had been adopted: see paragraph 57.

within the prescribed time the measures necessary to comply with the Directive.[7] It was against this backdrop that the 2011 Act was enacted.[8]

11. It is important to emphasize at the outset that the Plaintiff's challenge is limited to two elements of the 2011 Act: first, the Plaintiff claims that the 2011 Act involves general and indiscriminate retention of telecommunications metadata contrary to EU law as interpreted in *Tele2 Sverige/Watson*; secondly, the Plaintiff claims that the 2011 Act does not subject access to retained data to prior review by a court or independent administrative authority. Other features of the 2011 Act are not in issue. In particular, while the 2011 Act also applies to access to retained telecommunications data for the purposes of the safeguarding of the security of the State and the saving of human life, the Plaintiff's challenge is concerned solely with the retention of, and access to, telecommunications metadata for the purposes of fighting serious crime.[9]

III. The Questions Referred

12. In the Order for Reference, the Supreme Court has referred six questions for preliminary ruling.

The First, Second and Fourth Questions: Scope of Data Retention Regime under the 2011 Act

13. By its first question, the Supreme Court has asked whether a general or universal data retention regime – even subject to stringent restrictions on retention and access – is *per se* contrary to the provisions of Article 15 of Directive 2002/58/EC, as interpreted in light of the Charter.

14. By its second question, the Supreme Court has asked whether – in considering whether to grant a declaration of inconsistency of a national measure implemented pursuant to Directive 2006/24/EC, and making provision for a general data retention regime (subject to the necessary stringent controls on retention and/or in relation to access), and in particular in assessing the proportionality of any such regime – a national court is entitled to have regard to the fact that data may be retained lawfully by service providers for their own commercial purposes, and may be required to be retained for reasons of national security excluded from the provisions of Directive 2002/58/EC.

15. These questions must be considered alongside the fourth question. By this question, the Supreme Court has asked if a national court is obliged to declare the inconsistency of a national measure with the provisions of Article 15 of the Directive 2002/58/EC, if the

---

[7] Judgment of 26 November 2009, *Commission v. Ireland,* C-202/09, EU:C:2009:736.

[8] The 2011 Act has since been amended, in particular by section 89 of the Competition and Consumer Protection Act 2014 (permitting the Competition and Consumer Protection Commission to make disclosure requests where data are required for the prevention, detection, investigation or prosecution of a competition offence). In 2017, the then Government published the general scheme of draft legislation to replace the 2011 Act. In light of the continuing uncertainty around the compatibility of data retention legislation with EU law, particularly in light of *Tele2 Sverige/Watson*, this legislation has not yet been enacted.

[9] Reference, paragraph 1.1. See also the High Court Judgment [2018] IEHC 685, paragraphs 1.19 and 4.3.

national measure makes provision for a general data retention regime for the purpose of combating serious crime, and where the national court has concluded, on all the evidence available, that such retention is both essential and strictly necessary to the achievement of the objective of combating serious crime.

16. These questions all concern, in essence, whether a data retention that is general in scope is contrary to Article 15 of Directive 2002/58/EC, as interpreted in light of the Charter. For this reason, it is appropriate to consider these questions together.

17. As is clear from the judgment underpinning the Reference, the Supreme Court uses the terms 'universal' or 'general' retention of data in contradistinction to 'targeted' retention of data.[10] For the purposes of these observations, the Defendants will use the term 'general' retention to describe a regime where "*the type of data which is retained and is limited as to the time for which it can be retained, but the data retained is not limited or targeted by reference to persons, locations or the like*".[11]

18. In the Defendants' submission, a general data retention regime – of the kind found in the 2011 Act – is not contrary to EU law.

Legal Principles

19. The e-Privacy Directive – with which this Reference is concerned – particularises and complements the EU's general data protection regime (formerly Directive 95/46/EC, now the General Data Protection Regulation) in the field of the electronic communications. It makes provision for the confidentiality of electronic communications,[12] including specifically traffic data[13] and location data.[14] The Directive does not apply to activities falling outside the scope of EU law and "*in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law*".[15] Article 15(1) of the Directive allows Member States to "*adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC*". In particular, it provides that "*Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph*". National measures adopted in accordance with Article 15(1) have to comply with the general principles of Community law, including fundamental rights. Thus, Article 15(1) expressly recognizes that Member States may adopt data

[10] Supreme Court Judgment, paragraph 3.18.
[11] Supreme Court Judgment, paragraph 3.18.
[12] Article 5, e-Privacy Directive.
[13] Article 6, e-Privacy Directive.
[14] Article 9, e-Privacy Directive.
[15] Article 1(3), ePrivacy Directive. See also Article 3(2) of the Data Protection Directive.

retention measures for *inter alia* law enforcement and national security purposes but makes no further provision as to the form or model of data retention.

20. In light of the significant rise in electronic communications and the growing recognition of the value of communications data for law enforcement purposes, an increasing number of Member States adopted national data retention measures. It was against this backdrop that the EU Legislature adopted the Data Retention Directive in order to impose an obligation on all Member States – by way of derogation from the regime under the e-Privacy Directive – to adopt measures to ensure that the specified categories of telecommunications metadata were retained so that they could be made available for access by law enforcement authorities in specific cases and in accordance with national law. It is significant to recall that, in proposing this legislation, the Commission had considered but rejected alternative measures such as data preservation or 'quick freeze' systems on the basis that such measures were not as effective as a system of general retention.[16]

21. In its judgment in *Digital Rights Ireland*, this Court found that the retention of, and access to, retained telecommunications metadata constituted a serious interference with the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter. In assessing whether the Data Retention Directive complied with the principle of proportionality, the Court accepted that the retention of telecommunications metadata genuinely served objectives of general interest, specifically the fight against serious crime and terrorism in order to ensure public security.[17] According to the Court, retained telecommunications metadata were a *"valuable tool for criminal investigations"*[18] and data retention was *appropriate* for attaining the objective of fighting serious crime.[19] However, in assessing the necessity of the Directive, the Court noted that the Directive covered "*in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime*".[20] The Court also considered that the Directive had failed to lay down "*substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use*" as well as "*clear and precise rules*" governing the extent of the interference with fundamental rights, which the Court described as "*wide-ranging and particularly serious*".[21] Finally, the Court went on to identify certain safeguards which were lacking from the Directive. Having regard to "*all the foregoing considerations*", the Court concluded that the Data Retention Directive constituted a disproportionate interference with the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter.[22]

22. While the general scope of the retention regime established under the Data Retention Directive was an important factor in the Court's assessment of proportionality, it is clear from the judgment in *Digital Rights Ireland* that it was not on this ground alone

---

[16] Annex to the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, Extended Impact Assessment, SEC(2005) 1131, at 13.
[17] *Digital Rights Ireland & Others*, EU:C:2014:238, paragraphs 41-44.
[18] *Digital Rights Ireland & Others*, EU:C:2014:238, paragraphs 49-51.
[19] *Digital Rights Ireland & Others*, EU:C:2014:238, paragraph 49.
[20] *Digital Rights Ireland & Others*, EU:C:2014:238, paragraph 57.
[21] *Digital Rights Ireland & Others*, EU:C:2014:238, paragraphs 61-65.
[22] *Digital Rights Ireland & Others*, EU:C:2014:238, paragraphs 54-69.

that the Court declared the Directive invalid. As Advocate General Saugmandsgaard Øe later commented in his Opinion in *Tele2 Sverige/Watson*, "*...if a generalised data retention had, in and of itself, been sufficient to render Directive 2006/24 invalid, there would have been no need for the Court to examine – as it did in detail – the absence of the safeguards mentioned in paragraphs 60 to 68 of that judgment*".[23] Thus, while finding that the specific regime created under the Data Retention Directive was invalid, this Court in *Digital Rights Ireland* did not call into question the very concept of data retention itself; on the contrary, it expressly endorsed the appropriateness of data retention as a means of achieving the objectives pursued.

23. However, in its subsequent judgment in *Tele2 Sverige/Watson*, which concerned the validity of national data retention regimes in Sweden and the United Kingdom, this Court held that Article 15(1) of the e-Privacy Directive must be interpreted as precluding *"national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communications"*.[24] While recognizing that the effectiveness of the fight against serious crime might depend to a great extent on the use of modern investigation techniques, the Court considered that "*such an objective of general interest, however fundamental it may be*" could not in itself justify national legislation providing for the general and indiscriminate retention of all traffic and location data.[25] At the same time, the Court observed that Article 15(1) did *"not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary"*.[26] According to the Court, such legislation must lay down clear and precise rules governing the scope and application of such a data retention measure, must impose minimum safeguards against abuse, and, in terms of substantive conditions, must meet "*objective criteria, that establish a connection between the data to be retained and the objective pursued*".[27] More particularly, the Court continued:

> *....the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.*[28]

---

[23] Opinion of Advocate General Saugmandsgaard Øe of 19 July 2016, *Tele2 Sverige/Watson*, C-203/15 and C-698/15, EU:C:2016:572, paragraph 201.

[24] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 112.

[25] *Tele2 Sverige/Watson*, EU:C:2016:970, paragraph 103.

[26] *Tele2 Sverige/Watson*, EU:C:2016:970, paragraph 108 (emphasis added).

[27] *Tele2 Sverige/Watson*, EU:C:2016:970, paragraphs 109-111.

[28] *Tele2 Sverige/Watson*, EU:C:2016:970, paragraph 111.

Notwithstanding the insistence on objective evidence for any data retention measures, the Court did not refer to any evidence in support of its conclusion that this model of *"targeted retention"* was either an appropriate means of achieving the objective of fighting serious crime or an effective alternative to a general retention regime.[29] In particular, the Court did not identify the rational connection between targeted measures, typical of surveillance for preventive purposes of known suspects using known devices, and other aspects of the objective of fighting serious crime, including detection, investigation and prosecution, where frequently neither suspect nor device is known in advance.

24. In *Ministerio Fiscal*, the Court of Justice provided guidance on the requirements for access to retained data, and specifically subscriber data, in the context of criminal proceedings arising from the robbery of a mobile telephone.[30] In its judgment, the Court made no reference to the fact that the Spanish data retention legislation at issue, Ley 25/2007, was of general scope and application.[31] Nor did the Court confine its analysis of the Spanish law to its value as a "*preventive measure*", instead repeatedly considering as well the other important objectives of "*investigating, detecting and prosecuting*" (serious) criminal offences.

25. More recently, in a series of references from the United Kingdom, France and Belgium, the Court of Justice has been asked to revisit its conclusion in *Tele2 Sverige/Watson* that only a regime of targeted, as opposed to general, retention of telecommunications metadata is permissible under EU law. While the judgments of the Court have yet to be delivered, on 15 January 2020, Advocate General Campos Sánchez-Bordona delivered his Opinions in these cases. In broad terms, the Advocate General has recommended that the Court maintain its case-law and, on this basis, conclude that the national regimes in question – which provide for general models of retention – are precluded by Article 15(1) of the e-Privacy Directive.[32]

26. However, it is difficult to reconcile this conclusion with the Advocate General's assessment of targeted retention. In particular, in the main Opinion addressing this issue, in Case C-520/18, *Ordre des barreaux francophones et germanophone*, the Advocate General has identified significant problems with the model of targeted retention proposed by the Court in *Tele2 Sverige/Watson:*

---

[29] While the Opinion of Advocate General Saugmandsgaard Øe in *Tele2 Sverige/Watson* referred to 'targeted surveillance' at paragraph 201 and made reference to a number of studies which questioned the necessity of general retention, none of the studies referred to by the Advocate General in fact provides any support for the concept of targeted retention: instead, they either suggest data preservation as an alternative to data retention or simply highlight the issues identified by this Court with the particular data retention regime established under the Data Retention Directive: see Opinion of 19 July 2016 of Advocate General Saugmandsgaard Øe in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, EU:C:2016:572, paragraph 209, footnote 65.

[30] Judgment of 2 October 2018, *Ministerio Fiscal*, Case C-207/16, EU:C:2018:788.

[31] In his Opinion, Advocate General Saugmandsgaard Øe appeared to interpret the notion of targeted retention in *Tele2 Sverige/Watson* as referring to the specific measure seeking access to retained data, rather than the general framework of data retention legislation itself: Opinion of Advocate General Saugmandsgaard Øe of 3 May 2018 in *Ministerio Fiscal*, C-207/16, EU:C:2018:300, paragraphs 37 and 84.

[32] Opinion of Advocate General Campos Sánchez-Bordona dated 15 January 2020, Case C-520/18, *Ordre des barreaux francophones et germanophone and Others ("Ordre des barreaux")*, EU:C:2020:7. This was subject only to the qualification that, "*in truly exceptional situations, characterised by an imminent threat or an extraordinary risk justifying an official determination of an emergency situation in a Member State*", national legislation could provide for the possibility, for a limited period of time, of imposing as extensive and general an obligation to retain data as is considered indispensable: *Ordre des barreaux*, EU:C:2020:7, paragraph 105.

(i) First, "*the identification of a group of potential perpetrators would probably be insufficient if they used anonymization techniques or false identities. The choice of these groups could also lead to a general suspicion of certain segments of the population and be qualified as discriminatory, depending on the algorithm used*".

(ii) Secondly, "*selection by geographical criteria (which, in order to be effective, would require targeting areas that are not too narrow) poses the same and other problems, as indicated by the European Data Protection Supervisor during the hearing, insofar as it could stigmatise certain areas*".

(iii) Thirdly, "*there may be some contradiction between the preventive character of retention aimed at a specific public or geographical area and the fact that the perpetrators of the crimes are not known in advance, nor the place and date of their commission*".[33]

Simply put, a model of targeted retention would be ineffective in practice and objectionable in principle. In place of targeted retention, the Advocate General suggested a model of "*limited retention*", by reference to the categories of data retained, retention periods, and other safeguards.[34] However, having regard to the complexity of the issue and the need for a detailed regulatory framework, the Advocate General stressed that these choices are matters for the legislature, whether at Member State or EU level. Of course, such a model of "*limited retention*" is in substance a model of general data retention: to use the language of the Supreme Court, it is a regime where "*the type of data which is retained and is limited as to the time for which it can be retained, but the data retained is not limited or targeted by reference to persons, locations or the like*".[35]

27. In the Opinions in the *Privacy International* and *Quadrature du Net* references, the Advocate General maintained a similar approach.[36] The tension which underlies these Opinions is encapsulated in the following statement:

> *While it is difficult, it is not impossible to determine precisely and on the basis of objective criteria the categories of data that it is deemed essential to retain, and the circle of persons who are affected. It is true that the most practical and effective option would involve the general and indiscriminate retention of any data that might be collected by the providers of electronic communications services, but ... resolving the issue is not a matter of practical effectiveness but of legal effectiveness within the framework of the rule of law.*[37]

In other words, the Advocate General has invited the Court to maintain its position of principle in *Tele2 Sverige/Watson* notwithstanding his assessment that targeted as opposed to general retention is ineffective in practice as well as discriminatory in

---

[33] *Ordre des barreaux,* EU:C:2020:7, paragraphs 88 and 89.
[34] *Ordre des barreaux,* EU:C:2020:7, paragraph 92.
[35] Supreme Court Judgment, paragraph 3.18.
[36] Opinion of Advocate General Campos Sánchez-Bordona dated 15 January 2020, Joined Cases C-511/18 and C-512/18, *Quadrature du Net/French Data Network and Others*, EU:C:2020:6; Opinion of Advocate General Campos Sánchez-Bordona dated 15 January 2020, Joined Case C-623/17, *Privacy International*, EU:C:2020:5. See also Opinion of Advocate General Pitruzzella in C-746/18, *Prokuratuur,* EU:C:2020:18, paragraphs 54-56.
[37] *Quadrature du Net/French Data Network and Others*, EU:C:2020:6, paragraph 135; *Privacy International*, EU:C:2020:5, paragraph 39 (emphasis added).

principle. Against this backdrop, it is important to turn to the findings of fact which have been made by the Supreme Court.

The Findings of Facts made by the Supreme Court

28. In contrast to the position in the references from *Tele2 Sverige/Watson* onwards, in this Reference, the Supreme Court of Ireland has had the benefit of detailed evidence, including expert evidence, on the forms and feasibility of data retention. In accordance with settled case-law and the division of functions between the national court and the Court of Justice, it is the national court that has sole jurisdiction to assess and determine the facts in the context of proceedings under Article 267 TFEU.[38] The Court of Justice is empowered to rule on the interpretation or validity of provisions of EU law "*only on the basis of the facts which the national court puts before it*".[39]

29. The evidence in the national proceedings included international expert evidence on the use of data retention for law enforcement and national security purposes as well as evidence from senior members of An Garda Síochána not only on the Plaintiff's case but on the experience on the use and value of data retention in law enforcement and security generally. This evidence was in large part uncontroverted.[40]

30. This evidence has confirmed the extremely important role of retained data not only in the Plaintiff's case but also in the fight against serious crime and threats to national security more generally.[41] Such evidence may be important in exculpating or exonerating individuals as well as in identifying suspects unknown to the authorities.[42] Indeed, according to the Supreme Court, "*the detection of, in particular, certain categories of serious crime and the prosecution thereof is increasingly influenced by evidence such as that which was tendered in the criminal proceedings against Mr. D*".[43]

31. In relation to the models of data retention, the Supreme Court concluded that, while organised crime and terrorism may "*in some cases*" give rise to prior suspicion, "*the type of serious crime with which these proceedings is concerned rarely involves any circumstances which could reasonably be known to investigating authorities and which could lead to prior suspicion*".[44] Noting that cases of this kind "*frequently involve[d] serious offences against women, children and other vulnerable persons*", and indeed

---

[38] See e.g. judgment of 14 March 2017, *G4S*, C-157/15, EU:C:2017:203, paragraph 36; judgment of 24 February 2015, *Grünewald*, C-559/13, EU:C:2015:109, paragraph 32; judgment of 5 March 1995, *Brasserie du pêcheur*, C-46/93, EU:C:1996:79, paragraph 58; judgment of 13 May 1986, *Bilka-Kaufhaus*, C-170/84, EU:C:1986:204, paragraph 36; judgment of 29 April 1982, *Pabst & Richarz*, C-17/81, EU:C:1982:129, paragraph 12.

[39] See e.g. judgment of 25 October 2017, *POLBUD – WYKONAWSTWO*, C-106/16, EU:C:2017:804, paragraph 27; judgment of 16 June 2015, *Gauweiler and Others*, C-62/14, EU:C:2015:400, paragraph 15; judgment of 9 March 2010, *ERG and Others*, EU:C:2010:126, C-378/08, paragraph 42.

[40] Supreme Court Judgment, paragraph 4.1.

[41] Reference, paragraphs 7.1-7.7. See, in this regard, the observations of Chief Justice Clarke in the Supreme Court Judgment, paragraph 6.5.

[42] Supreme Court Judgment, paragraph 4.2.

[43] Reference, paragraph 8.2 (emphasis added). This is consistent with the observation of the Advocate General in *Ordre des barreaux* that "*[t]he justification for the obligation for providers of electronic communications services to retain certain data, and not only for the management of their contractual obligations to users, is increasing in line with technological developments*": *Ordre des barreaux,* EU:C:2020:7, paragraph 81.

[44] Reference, paragraph 8.3.

that telephony was often used "*for the purposes of grooming or otherwise exploiting vulnerable persons*", the Supreme Court found that, in a significant number of such cases, "*it would not be possible to detect, let alone adequately prosecute, the perpetrator*" and, in other cases, the ability to mount a successful prosecution "*would be severely impaired*" if law enforcement authorities did not have access to telecommunications metadata.[45] The Supreme Court expressed the position starkly: if general retention were not permissible, "*it follows that many of these serious crimes against women, children and other vulnerable persons will not be capable of detection or successful prosecution*".[46]

32. Against that background, the Supreme Court made the following critically important findings of fact:-

    (i) Alternative forms of data retention, by means of geographical targeting or otherwise, would be ineffective in achieving the objectives of the prevention, investigation, detection and prosecution of at least certain types of serious crime, and further, could give rise to the potential violation of other rights of the individual;[47]

    (ii) The objective of the retention of data by any lesser means than that of a general data retention regime, subject to the necessary safeguards, is unworkable; and

    (iii) The objectives of the prevention, investigation, detection and prosecution of serious crime would be significantly compromised in the absence of a general data retention regime.

    In short, on the basis of the detailed body of evidence adduced before it (much of which was undisputed, the Supreme Court has concluded that targeted retention would be ineffective as a law enforcement tool and indeed could itself be incompatible with fundamental rights. According to the Court, data retention is only effective as a law enforcement tool if it is general in scope at the retention stage. In the words of the Supreme Court, "*it is not possible to access that which has not been retained*".[48]

Proportionality of a General Data Retention Regime

33. It is in light of these findings of fact that the Court must address the first, second and fourth questions and, in particular, assess the question of the compatibility of a general data retention regime with EU law.

---

[45] Reference, paragraph 8.4.
[46] Reference, paragraph 8.5.
[47] Indeed, in the Supreme Court judgment, the Supreme Court expressed its concern about any model of targeted retention, describing it as "*troubling from the perspective of Irish constitutional law and the analysis which an Irish court would apply under the Constitution, the Convention and the Charter*": Supreme Court Judgment, paragraph 6.15. According to the Supreme Court, it was apparent "*both as a matter of logic and as established by the evidence in this case, that any such measure cannot achieve the objective of permitting the investigation of serious crimes such as the subject matter of these proceedings, where there is no reason to suspect a particular individual or group in advance*": Supreme Court Judgment, paragraph 6.16.
[48] Reference, paragraph 8.5.

34. As already noted, Article 15(1) of the e-Privacy Directive expressly provides that Member States may adopt data retention measures. In its jurisprudence, this Court has never sought to suggest that data retention *per se* is incompatible with the Charter of Fundamental Rights. As expressed by the Supreme Court, such a conclusion would be "*a value judgment but one not apparent from the Charter nor, it would appear, one which would be made either under the Convention or the Irish Constitution*".[49] In circumstances where data retention can only be effective as a law enforcement and national security tool if it is general in scope at the retention stage, it must follow that a general retention regime, such as that found in the 2011 Act, cannot be precluded by Article 15(1) of the e-Privacy Directive, read in light of the Charter. While such a regime may be general in scope, it cannot properly be described as indiscriminate.

35. In assessing the proportionality of the 2011 Act for the purposes of Article 52 of the Charter, it is important to emphasize the following considerations.

36. First, the Irish data retention regime is clearly "*provided for by law*" in the form of the 2011 Act.

37. Secondly, while it is accepted that data retention constitutes a serious interference with Articles 7 and 8 of the Charter in particular,[50] the Court has confirmed that data retention does not infringe the essence of these rights.[51] In this regard, it must be recalled that the rights guaranteed in Articles 7 and 8 "*are not absolute rights, but must be considered in relation to their function in society*".[52]

38. Thirdly, this Court has recognised that data retention genuinely meets an important objective of general interest in the fight against crime, including organised crime and terrorism, in order to ensure public security, and in this context has also had regard to the right to security in Article 6 of the Charter.[53] However, drawing on its "*very considerable experience*" of balancing privacy rights with the requirements of the fight against crime,[54] the Supreme Court has emphasized that due weight must also be accorded to the rights of victims of crime under the Irish Constitution and to the positive obligations of States under Articles 2, 3, 4 and 8 of the European Convention of Human Rights.[55] In this regard, it is relevant to note that, in his Opinion in *Ordre des barreaux*, Advocate General Campos Sánchez-Bordona has also referred to the guarantees enshrined in *inter alia* Articles 1, 2, 3 and 4 of the Charter.[56] In other words, in assessing the proportionality of data retention measures in accordance with Article 52 of the Charter, it is necessary to have regard not only to the "*objectives of general interest*

---

[49] Supreme Court Judgment, paragraph 6.16.

[50] In its judgment in *Tele2 Sverige*/Watson, the Court also made reference to the freedom of expression guaranteed under Article 11 of the Charter: see *Tele2 Sverige/Watson*, EU:C:2016:970, paragraphs 92-93 and 101.

[51] *Digital Rights Ireland & Others*, EU:C:2014:238, paragraphs 39-40; *Tele2 Sverige/Watson*, EU:C:2016:970, paragraph 101.

[52] See e.g. judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraph 48; Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 136; judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, paragraph 172.

[53] See especially *Digital Rights Ireland & Others*, EU:C:2014:238, paragraphs 42-43. In the words of the Supreme Court, this objective is "*a lawful and permissible objective of considerable weight in any society governed by the rule of law*": Supreme Court Judgment, paragraph 6.8.

[54] Supreme Court Judgment, paragraph 6.4.

[55] Supreme Court Judgment, paragraphs 6.9-6.13.

[56] *Ordre des barreaux*, EU:C:2020:7, paragraphs 114-118.

recognised by the Union" but also "*the need to protect the rights and freedoms of others*".

39. Fourthly, in *Digital Rights Ireland*, the Court recognised the appropriateness of data retention as a means of achieving the objectives of fighting serious crime and threats to public security. It did so in the context of a general data retention regime of the kind required by the Data Retention Directive. By contrast, in light of the Supreme Court's findings of fact, it is clear that a model of targeted retention – of the kind proposed by the Court in *Tele2 Sverige/Watson* – would not be an appropriate means of achieving these objectives on account of its lack of effectiveness, in particular as regards the "*investigation, detection and prosecution*" of serious criminal offences. Indeed, such a model is also likely to be "*more intrusive of the rights of the individuals concerned*" than general retention.[57]

40. Fifthly, and finally, in considering the necessity of data retention *stricto sensu*, it is particularly important to emphasize the Supreme Court's finding that the objectives pursued by data retention could not be achieved by "*any lesser means than that of a general data retention regime*" and would be "*significantly compromised in the absence of a general data retention regime*". In other words, the objectives cannot be attained by other appropriate and less restrictive measures.[58] In light of this finding, there is no basis for the conclusion that a general data retention regime is *per se* disproportionate and precluded by Article 15(1) of the e-Privacy Directive.

41. This conclusion is reinforced when one considers the referring court's second question. In the Defendants' submission, in considering the validity of the data retention regime under the 2011 Act, the Supreme Court is entitled to have regard to the fact that data may be retained lawfully by service providers for their own commercial purposes, and may also be required to be retained for reasons of national security.

42. First, if it is possible for the electronic communications service providers to retain telecommunications metadata for their own commercial purposes – including billing, marketing and the provision of value added services[59] – it is difficult to justify the proposition that such data can never be retained for other compelling public interests, particularly where electronic communications are themselves increasingly means of committing serious crimes and engaging in threats to public security.[60] However, the fact that such data are retained for commercial purposes does not obviate the need for a legal framework requiring the retention of such data for law enforcement and national security purposes. In the absence of such a framework, certain categories of data – such as location data which is especially valuable in the fight against terrorism and serious

---

[57] Supreme Court Judgment, paragraph 6.15.

[58] See e.g. judgment of 2 April 2020, *Ruska Federacija*, C-897/19 PPU, EU:C:2020:262, paragraph 60; judgment of 6 September 2016, *Petruhhin*, C-182/15, EU:C:2016:630, paragraphs 37-38; judgment of 16 July 2015 in *CHEZ Razpredelenie Bulgaria*, C-83/14, EU:C:2015:480, paragraphs 120 to 122. See also Opinion of Advocate General Saugmandsgaard Øe of 19 July 2016, *Tele2 Sverige/Watson*, C-203/15 and C-698/15, EU:C:2016:572, paragraph 185.

[59] Articles 6(2), (3) and (6) and Article 9(3), Directive 2002/58/EC.

[60] *Ordre des barreaux*, EU:C:2020:7, paragraph 81 ("... *it would not seem logical to limit it to the mere exploitation of the data that operators retain for the exercise of their commercial activities and only for the time necessary for those activities*").

crime (as for example in the Plaintiff's case) – would only be retained by service providers in aggregate form for their own commercial purposes.[61]

43. Secondly, Member States may also adopt data retention measures in the field of national security which remains, in accordance with Article 4(2) TEU, "*the sole responsibility of each Member State*".[62] Having regard to the particular nature of the threats facing Member States in this field, the Supreme Court's findings would apply *a fortiori* in this context. Indeed, in his Opinion in *Ordre des barreaux*, the Advocate General recognised that such threats may justify, by way of exception, data retention measures of general scope.[63] If there is a general obligation to retain telecommunications metadata for national security purposes, such that the relevant data are in any event retained, it becomes even more difficult to sustain a claim that a general obligation to retain metadata for the purpose of fighting serious crime is *per se* disproportionate and impermissible, all the more so where the objective evidence supports the conclusion that general retention is not merely the least intrusive but the only means of attaining this objective.

44. While it is accepted that retention and access constitute distinct interferences with Articles 7 and 8 of the Charter, these considerations also demonstrate why a strict distinction between retention and access in the assessment of proportionality is not "*necessarily helpful or indeed truly possible*".[64] As the Supreme Court has observed, it is clear that the objective of retention "*is to permit access*" and it is "*only when access is sought and obtained that it is possible to connect an individual to any specific retained data*". In this sense, the interference with fundamental rights which retention in itself entails – important though it may be – is limited and can only be meaningfully assessed in light of the arrangements in place for access.

Conclusion on the First, Second and Fourth Questions

45. For all these reasons, the Defendants submit that the first question must be answered in the negative: a general data retention regime is not *per se* contrary to Article 15 of Directive 2002/58/EC, interpreted in light of the Charter. If the Court were to conclude otherwise, it would be tantamount to prohibiting the use of data retention as a law enforcement tool despite its vitally important and increasingly relevant role in the fight against serious crime, in particular in the investigation, detection and prosecution of serious crimes, and threats to national security.

---

[61] Significantly, on the facts of the present case where such data played a highly significant role, the evidence before the national court confirmed the service providers do not retain location data except in aggregate form.

[62] The precise extent to which national security falls outside the scope of the e-Privacy Directive is at issue in the pending references in Cases C-623/17, *Privacy International*, C-511/18 and C-512/18, *Quadrature du Net & Others* and C-520/18, *Ordre des barreaux*. In his Opinions in these cases, Advocate General Campos Sánchez-Bordona has advised the Court to conclude that national data retention legislation for national security purposes falls within the scope of EU law: see *Quadrature du Net/French Data Network and Others*, EU:C:2020:6, paragraph 42.

[63] *Ordre des barreaux*, EU:C:2020:7, paragraph 105.

[64] Supreme Court Judgment, paragraph 6.6. Further, as the Supreme Court observed, "*any individual concerned must necessarily be aware of the fact both that data is generated and may be retained by operators for their own commercial purposes and may be available for lawful access during that period*": Supreme Court Judgment, paragraph 6.7. Indeed, the expert evidence before the national court questioned the appropriateness of term 'surveillance' to describe the mere retention of telecommunications data: Reference, paragraph 7.4.

46. With respect to the second question, in assessing the validity of a national data retention regime, a national court is entitled to have regard to the fact that data may be retained lawfully by service providers for their own commercial purposes, and may also be required to be retained for reasons of national security.

47. With respect to the fourth question, where the national court has concluded, on all the evidence available, that a general data retention regime is both essential and strictly necessary to the achievement of the objective of combating serious crime, a national court cannot be obliged to declare the inconsistency of a national measure with the provisions of Article 15 of the Directive 2002/58/EC.

48. Any other conclusion would compel the referring court to reach a conclusion which runs contrary to evidence in a manner which could not be reconciled with the division of functions between this Court and the national courts under Article 267 TFEU or indeed with the concept of a Union based on the rule of law.

The Third Question: the Access Regime under the 2011 Act

49. By its third question, the Supreme Court has asked – in the context of determining the compatibility of a national measure for access to retained data with European Union law and in particular with the Charter – what criteria a national court should apply in considering whether any such access regime provides the required independent prior scrutiny as determined by this Court in its case-law. In that context, the Supreme Court has asked whether a national court, in making such an assessment, can have any regard to the existence of *ex post* judicial or independent scrutiny.

Legal Principles

50. First, it is important to recall that, while Article 15(1) of the e-Privacy Directive permits Member States to adopt data retention measures subject to certain conditions, it makes no reference to access by competent authorities to retained data, whether for law enforcement, national security or other purposes. This reflects the fact that, in accordance with Article 1(3), the e-Privacy Directive does not apply to the activities of the State in these fields. In a similar way, when the EU legislature adopted the Data Retention Directive, it did so without prejudice to the power of Member States to adopt measures concerning access to retained data which was expressly recognised as falling outside the scope of Community law.[65] Indeed, in this Court's judgment in *Ireland v. Parliament & Council*, one of the main grounds on which the Court upheld the validity of Article 95 EC as the legal basis for the Directive was that its provisions were "*essentially limited to the activities of service providers*" and did not "*govern access to data or the use thereof by the police or judicial authorities of the Member States*".[66] It follows that there have never been any legislative rules at EU level defining the conditions governing access to retained data, still less the specific body charged with prior review of access requests.

---

[65] Directive 2006/24/EC, recital 25. This was reflected in Article 4 of the Directive which simply required that Member States adopt measures to ensure that "*data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law*".

[66] *Ireland v Parliament and Council*, C-301/06, EU:C:2009:68, paragraph 80.

51. Of course, in this Court's judgment in *Digital Rights Ireland*, the Court concluded that the failure on the part of the EU legislature to lay down clear and precise rules in relation to access to retained data was one of the primary reasons why the Directive constituted a disproportionate interference with Articles 7 and 8 of the Charter of Fundamental Rights. In identifying the lack of safeguards around access, the Court observed that the Directive did not itself lay down – or require Member States to lay down – any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. "*Above all*", the Court stated, "*the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions*".[67]

52. In *Tele2 Sverige/Watson*, the Court reiterated this requirement, this time in the context of national data retention regimes. According to the Court, national legislation must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. The Court continued:

> *In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 62; see also, by analogy, in relation to Article 8 of the ECHR, ECtHR, 12 January 2016, Szabó and Vissy v. Hungary, CE:ECHR:2016:0112JUD003713814, §§ 77 and 80).*[68]

While laying down this general but not absolute requirement, the Court did not identify the criteria for determining what constitutes an independent administrative authority or body for this purpose.

53. The Court did, however, make reference to the relevant case-law of the European Court of Human Rights and specifically its judgment in *Szabó and Vissy v. Hungary*. While recognising the important role of independent prior authorisation, the Strasbourg Court has stopped short of imposing any general requirement of prior judicial authorisation, except in the special case of the confidentiality of journalist's sources,[69] even in the context of surveillance measures which are much more far-reaching in their

---

[67] *Digital Rights Ireland & Others*, EU:C:2014:238, paragraph 62.
[68] *Tele2 Sverige/Watson*, EU:C:2016:970, paragraph 120. See also Opinion 1/15, EU:C:2017:592, paragraphs 197-223.
[69] *Telegraaf Media & Others v Netherlands* [2012] ECHR 1965.

interference with fundamental rights than data retention.[70] Moreover it is clear from this case-law that the Strasbourg Court's concern is that authorisation of measures involving an interference with the right to privacy should not be subject to political interference and that the authorising authority is, in this sense, "*sufficiently independent from the executive*".[71] The Court has also underlined the role and importance of *post factum* judicial oversight in this regard.[72]

54. In the pending reference in Case C-746/18, *Prokuratuur*, the Estonian Supreme Court has asked this Court whether the Public Prosecutor's Office in Estonia may be considered to be an independent administrative authority within the meaning of the judgment in *Tele2 Sverige/Watson*. In Estonia, the Public Prosecutor's Office – which enjoys a statutory guarantee of independence and is obliged to act in accordance with the law – directs the pre-trial procedure in the course of which access to retained data may be sought and also brings the prosecution before the court if this is warranted. While the judgment of the Court is awaited, in his Opinion of 21 January 2020, Advocate General Pitruzzella has advised that the requirement of prior review by a court or independent administrative authority is not met "*where national legislation provides that such review is to be carried out by the public prosecutor's office which is responsible for directing the pre-trial procedure, whilst also being likely to represent the public prosecution in judicial proceedings*".[73] According to the Advocate General, the dual role of the public prosecutor's office may "*raise legitimate doubts as to the ability of the public prosecutor's office to carry out a neutral and objective prior review of the proportionality of the access to data ...*".[74] The Advocate General also expressed the view that a lack of prior independent review could not be "*offset by carrying out a judicial review after access has been granted*" as "*[o]therwise the prior nature of the review would lose its purpose*".[75] However, the Advocate General emphasized that it was in principle for Member States to determine and implement their own measures to ensure prior review of access requests.[76]

The System of Prior Review under the 2011 Act

55. As the Reference makes clear, in the Plaintiff's case, "*there was no suggestion either at his criminal trial or in these proceedings that the specific manner in which the legislation was operated in the particular circumstances of this case was abusive or inappropriate*".[77] Notwithstanding this position, the Plaintiff maintains a challenge, in principle, to the system of prior review of access requests under the 2011 Act.

---

[70] *Kennedy v. United Kingdom* [2010] ECHR 682, paragraph 167; *Zakharov v. Russia* (2016) 63 EHRR 17, paragraph 258 and 275; *Szabo and Vissy v. Hungary* (2016) 63 EHRR 3, paragraph 77.
[71] *Szabo and Vissy v. Hungary* (2016) 63 EHRR 3, paragraph 77.
[72] *Szabo and Vissy v. Hungary* (2016) 63 EHRR 3, paragraphs 77-80.
[73] Opinion of Advocate General Pitruzzella of 20 January 2020, *Prokuratuur*, C-746/18, EU:C:2020:18, paragraph 129.
[74] *Prokuratuur*, EU:C:2020:18, paragraph 118.
[75] *Prokuratuur*, EU:C:2020:18, paragraph 128.
[76] *Prokuratuur*, EU:C:2020:18, paragraph 127.
[77] Reference, Appendix II, paragraph 4. Indeed, the High Court had concluded "*the Plaintiff has not established for this Court that the actual operation of the 2011 Act from retention in November 2011 to the date of disclosure in October 2013 for telephony data of the 407 number was inappropriate, unnecessary or disproportionate*": High Court Judgment, paragraph 5.17.

56. For the purposes of the 2011 Act, the Commissioner of An Garda Síochána, the Irish police force, has established "*a small, independent unit known as the Telecommunications Liaison Unit*" ("TLU") under the direction of a senior member of An Garda Síochána, which has responsibility for carrying out prior review of requests for access to retained data.[78] Members of An Garda Síochána seeking access to retained telecommunications metadata for the purposes of investigating a serious offence must obtain approval in the first instance from their superintendent. If approved, a reasoned request is sent to the TLU. The TLU and the detective chief superintendent in charge of the TLU are required to "*verify the legality, proportionality and necessity of disclosure requests*" and applications which do not comply with the law or internal protocols are returned to the requesting officers.[79] As confirmed by the Supreme Court on the basis of the evidence before it, "*the TLU and the relevant Detective Chief Superintendent operate independently of the investigatory functions of An Garda Síochána*".[80]

57. This system of prior review is reinforced by a multi-layered *ex post facto* review. First, the TLU is subject to audit by the Data Protection Commissioner.[81] Secondly, under section 10 of the 2011 Act, a person who believes that their data has been accessed under the Act may refer a complaint for investigation to the Complaints Referee, who is a serving judge of the Circuit Court. Thirdly, under section 12 of the 2011 Act, the designated judge – who is a judge of the High Court – is required to keep the operation of the Act under review and to ascertain whether the authorities are complying with its provisions. For this purpose, the designated judge has the power to investigate any disclosure request made, and to access and inspect any relevant document or record.[82] Fourthly, insofar as any evidence obtained under the 2011 Act is relied upon in a criminal prosecution, it is liable to come "*under intense scrutiny in the context of the criminal trial*" and in fact did so in the case of the prosecution of GD for murder.[83]

Assessment of the System of Prior Review under the 2011 Act

58. At the outset, it is important to recall that neither Article 15(1) of the e-Privacy Directive nor the Charter provides guidance on the criteria which must be satisfied by an independent administrative authority in this specific context. The concept of an independent administrative authority is not a concept found either in the Treaties or in EU legislation which must, in consequence, enjoy a uniform or autonomous meaning in EU law.

59. What is clear is that an independent administrative authority does not need to be a court or, in the language of Article 47 of the Charter, "*an independent and impartial tribunal*".[84] While a Member State may choose to vest the prior review function in a court or tribunal, a Member State is equally entitled to vest this function in an

---

[78] Reference, paragraph 3.4.
[79] Reference, paragraph 3.5.
[80] Supreme Court Judgment, paragraph 3.21.
[81] Reference, paragraph 3.5; section 4(2), Communications (Retention of Data) Act 2011.
[82] Reference, Appendix I, paragraph 8; section 12(2), Communications (Retention of Data) Act 2011.
[83] Supreme Court Judgment, paragraph 6.21.
[84] On the requirements of independence for the courts, see e.g. judgment of 25 July 2018, *Minister for Justice and Equality (Deficiencies in the system of justice)*, C-216/18 PPU, EU:C:2018:586; judgment of 24 June 2019, *Commission* v *Poland (Independence of the Supreme Court)*, C-619/18, EU:C:2019:531; judgment of 5 November 2019, *Commission* v *Poland (Independence of the ordinary courts)*, C-192/18, EU:C:2019:924.

administrative body once that body is independent in the exercise of this function. While the jurisprudence of the Court on the requirement of independence in other contexts may provide some useful guidance on its meaning that jurisprudence cannot simply be transposed to this distinct context without nuance or qualification.

60. For example, in the field of data protection, Article 8(3) of the Charter requires that compliance with the rules in Article 8 "*shall be subject to control by an independent authority*". In accordance with Article 52 GDPR, each supervisory authority "*shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation*". The Court has emphasized that this requirement of complete independence means that a supervisory authority must enjoy "*operational independence*" in the sense that they are able to perform its duties "*free from external influence*", in whatever form, direct or indirect.[85] In addition, there must be no risk of political influence over the supervisory authority's decision-making which could undermine the requirement to "*remain above all suspicion of partiality*".[86] Of course, an independent authority for the purposes of Article 8(3) of the Charter and the GDPR performs wide-ranging supervisory and enforcement functions, and is vested with extensive corrective powers, for the purposes of protecting individual rights. Indeed, as noted above, Ireland's Data Protection Commission has an express supervisory function under the 2011 Act. However, this role is quite different from that carried out by an independent authority charged with the much more discrete function of prior review of access requests.

61. The Court has also provided guidance on the requirement of independence in the context of the issuing judicial authority under the European Arrest Warrant regime.[87] Against the backdrop of diverse national criminal justice systems, the Court has emphasized the need to undertake a specific assessment as to whether an authority in any particular jurisdiction is capable "*of exercising its responsibilities objectively, taking into account all incriminatory and exculpatory evidence, without being exposed to the risk that its decision-making power be subject to external directions or instructions, in particular from the executive, ...*".[88] While this guidance may be of some assistance, it must again be borne in mind that the issuing judicial authority serves a very different function and operates within a distinct legislative framework to that of an authority charged with prior review of access requests.

62. In the case of the 2011 Act, it is clear that, while the body charged with prior review of access requests, the TLU, forms part of An Garda Síochána, it is operationally and

---

[85] See judgment of 9 March 2010, *Commission v. Germany*, C-518/07, EU:C:2010:125, paragraph 30; judgment of 16 October 2012, *Commission* v *Austria,* C-614/10, EU:C:2012:631, paragraph 41; and judgment of 8 April 2014, *Commission v. Hungary*, C-288/12, EU:C:2014:237, paragraph 51.

[86] See judgment of 9 March 2010, *Commission v. Germany*, C-518/07, EU:C:2010:125, paragraph 36; judgment of 16 October 2012, *Commission v Austria*, C-614/10, EU:C:2012:631, paragraph 52; and judgment of 8 April 2014, *Commission v. Hungary*, C-288/12, EU:C:2014:237, paragraph 53.

[87] In contrast to the concept of an independent administrative authority at issue in this case, the concept of an issuing judicial authority is the subject of specific EU legislation and must therefore enjoy an "*autonomous and uniform interpretation*" throughout the E: see judgment of 27 May 2019, *OG and PI*, Joined Cases C-508/18 and C-82/19 PPU, paragraph 73.

[88] *OG and PI*, C-508/18 and C-82/19 PPU, paragraph 73. See also judgment of 12 December 2019, *JR and YC*, C-566/19 PPU et C-626/19 PPU, paragraph 56.

functionally independent. There is no question of the TLU being subject to executive or political interference. As the Supreme Court has confirmed, the role of the TLU is independent from the investigatory role of An Garda Síochána and the TLU officers, who are duty-bound to verify the legality, proportionality and necessity of all access requests, are not involved in the conduct of criminal investigations. In this sense, the position of the TLU is distinguishable from that of the Public Prosecutor's Office at issue in Case C-746/18, *Prokuratuur*.[89] Moreover, as the jurisprudence of the Strasbourg Court makes clear, it is necessary and appropriate to have regard to the extensive mechanisms for *post factum* oversight, including judicial oversight, under the 2011 Act.[90] These mechanisms serve to reinforce the objectivity, reliability and effectiveness of the system of prior review.

63. In circumstances where its operational and functional independence is beyond doubt, the mere fact that the TLU forms part of An Garda Síochána should not automatically exclude it from being considered an independent administrative authority for present purposes. Indeed, in carrying out its tasks, the TLU draws on an expertise and understanding of the process of criminal investigation which arguably permits a more robust and effective scrutiny of requests than might be carried out by a court charged with this function.[91] In his Opinion in Case C-746/18, Advocate General Pitruzzella did not accept the Commission's argument that measures of internal administrative organisation could overcome the shortcomings in the independence of the Estonian Public Prosecutor's Office on the facts of that particular case, on account of the hierarchical organisation of the Office. However, in reaching that conclusion, the Advocate General did not exclude this possibility in other cases, observing that "*having an institution with an outside view on the interests relating to the proceedings in question must not be at the expense of weakening the effectiveness of the investigation, detection and prosecution of criminal offences*".[92]

64. Indeed, in the Opinion in Case C-746/18, the Advocate General advised that, in order to respect the procedural autonomy of the Member States, "*the Court should not interfere further with the general organisation of the administration of justice in Member States...*".[93] This consideration is particularly important in circumstances where there are no legislative rules at EU level on this issue, and where the issue raises sensitive questions about the organisation of, and division of functions within, Member States' systems for law enforcement and the administration of justice. In this context, Member States must be afforded an appropriate margin of discretion in the development of their national systems for prior review of access. Otherwise, there is a real risk that

---

[89] Thus, to use the language of that Opinion, the TLU is "*not directly involved in the criminal investigation*" and "*could not be criticized for wanting to put the interests of the investigation first at the expense of those linked to the protection of the data of the persons concerned*": *Prokuratuur*, EU:C:2020:18, paragraph 126.

[90] *Szabo and Vissy v. Hungary* (2016) 63 EHRR 3, paragraph 77; *Kennedy v. United Kingdom* [2010] ECHR 682, paragraph 167. This has been considered as an important factor in the CJEU's assessment of complaints that the European Commission, in competition cases, acted as prosecutor and adjudicator contrary to Article 6 ECHR: see e.g. T-348/94, *Enso Espanola*, EU:T:1998:102, paragraphs 60-65; *KME Germany v Commission*, C-272/09 EU:C:2011:63/810, paragraphs 91-106.

[91] The expert evidence before the High Court was to the effect that the UK system under which police officers independent of an investigation conducted the prior review of access requests was regarded as providing "*robust and effective pre-authorisation scrutiny as well as a measure of independence*", with police officers rejecting more applications than lay magistrates.

[92] *Prokuratuur*, EU:C:2020:18, paragraph 126.

[93] *Prokuratuur*, EU:C:2020:18, paragraph 127.

matters which are appropriate for legislative intervention tailored to the requirements of Member States' diverse criminal justice systems would be regulated by judicially crafted rules developed on a piecemeal basis at EU level according to the vagaries of litigation.

65. For all these reasons, it is submitted that the system of prior review provided for under the 2011 Act satisfies the requirement for prior review of access by an independent administrative body laid down by this Court in *Digital Rights Ireland* and *Tele2 Sverige/Watson.* What is essential in this regard is that the TLU is operationally and functionally independent and free of any political or government influence in the exercise of this function. Moreover, the mechanism of prior review is reinforced by important mechanisms of *post factum* review.

The Fifth and Sixth Questions: the Temporal Effect of Any Declaration of Inconsistency with EU Law

66. By its fifth question, the Supreme Court has asked whether a national court – which is obliged to conclude that a national measure is inconsistent with the provisions of Article 15 of Directive 2002/58/EC, as interpreted in the light of the Charter – is entitled to limit the temporal effect of any such declaration, if satisfied that a failure to do so would lead to "*resultant chaos and damage to the public interest*".[94]

67. By its sixth question, the Supreme Court has asked whether a national court invited to declare the inconsistency of national legislation with Article 15 of the Directive 2002/58/EC, and/or to disapply this legislation, and/or to declare that the application of such legislation had breached the rights of an individual, either in the context of proceedings commenced in order to facilitate an argument in respect of the admissibility of evidence in criminal proceedings or otherwise, may be permitted to refuse such relief in respect of data retained pursuant to the national provision enacted pursuant to the obligation under Article 288 TFEU to faithfully introduce into national law the provisions of a directive, or to limit any such declaration to the period after the declaration of invalidity of the Directive 2006/24/EC issued by the CJEU on the 8th day of April, 2014.

68. As these questions both relate to the power of national courts to limit the effects of any declaration of inconsistency of national law with EU law, it is appropriate to consider the fifth and sixth questions together. For the reasons set out above, it is submitted that the first to fourth questions do not disclose any inconsistency with EU law. However, in the event that the national court were to conclude otherwise, the Defendants make the following submissions.

Legal Principles

[94] The Supreme Court describes this as being in line with the approach taken, for example, in *R (National Council for Civil Liberties) v Secretary of State for Home Department and Secretary of State for Foreign Affairs* [2018] EWHC 975, at para. 46.

69. In accordance with settled case-law, it is in principle for the national court to determine the consequences of the incompatibility of domestic legislation with EU law in the domestic legal system.[95] In the judgment in *Liberty* referred to in the Supreme Court's fifth question, the High Court of England Wales did precisely that. Having concluded that Part 4 of the Investigatory Powers Act 2016 was inconsistent with EU law in two respects,[96] the High Court granted a declaration of inconsistency with EU law but suspended its effect for a reasonable period of time in order to give Parliament an opportunity to amend that legislation so as to bring it in line with EU law.[97] The Court took this step because of its concern that immediate disapplication of the legislation would have resulted in "*chaos and damage to the public interest*".[98] The practical implications of immediate disapplication would, in the Court's view, have been "*enormous and potentially damaging to the public interest*".[99]

70. Of course, in determining the consequences of inconsistency of domestic legislation with EU law, a national court may draw guidance from the approach of the Court of Justice to the consequences of invalidity of EU legislation. Even in cases where the Court of Justice declares an instrument of Union law void or invalid,[100] the Court has jurisdiction to limit the effects, including the temporal effects, of any such declaration.[101] In appropriate cases, the Court has suspended the effects of its declaration in order to allow the EU legislature to adopt new legislation that addresses the Court's concerns.[102] Thus, while in theory a declaration by the Court of Justice that an instrument of EU law is void or invalid has retrospective effect,[103] the Court has often limited the temporal effect of such a declaration in the interests of legal certainty where the circumstances of the particular case so require.[104]

71. Thus, for example, in the *Defrenne* case, in the face of arguments from Member States that the retrospective recognition of direct effect of Article 119 EC would have serious financial consequences, the Court of Justice – on the basis of "*important considerations of legal certainty affecting all the interests involved, both public and private*" – held that its ruling could not be relied on in order to support claims concerning pay periods

---

[95] Judgment in *Paint Graphos and Others*, C-78/08 to C-80/08, EU:C:2011:550, paragraph 34; Judgment in *Hünermund and Others*, C-292/92, EU:C:1993:932, paragraph 8.

[96] *R (National Council for Civil Liberties) v Secretary of State for Home Department and Secretary of State for Foreign Affairs* [2018] EWHC 975 ('*Liberty*'), paragraphs 186-187. First, access to retained data was not limited to the purpose of combating serious crime and, secondly, access was not subject "to prior review by a court or an independent administrative body.

[97] *Liberty*, paragraphs 186-187.

[98] *Liberty* [2018] EWHC 975, paragraph 46.

[99] *Liberty* [2018] EWHC 975, paragraph 77.

[100] Under the annulment procedure, the Court of Justice can declare acts of the Union "*void*": Article 264 TFEU. Article 267 TFEU confers jurisdiction on the Court to rule on the "validity" of Union acts.

[101] Indeed, in the context of annulment actions, Article 264 TFEU provides that, if the Court declares an act void, the Court "*shall, if it considers this necessary, state which of the effects of the act which it has declared void shall be considered as definitive*".

[102] See e.g. Judgment of 3 September 2008 in *Kadi and Al Barakaat International Foundation v Council and Commission,* C-402/05 P, EU:C:2008:461, paragraphs 373-376. These principles have been applied by way of analogy in the context of declarations of invalidity in preliminary reference proceedings brought under Article 267 TFEU: Lenaerts, Maselis and Gutman, *EU Procedural Law* (OUP, 2014), paragraph 10.22.

[103] Judgment of 26 April 1994 in *Roquette Freres*, C-228/92, EU:C:1994:168, paragraph 17; Judgment of 12 June 1980 in *Express Dairy Foods*, Case 130/79, EU:C:1980:155, paragraph 14.

[104] Judgment of 22 December 2008 in *Société Régie Networks*, C-333/07, EU:C:2008:76, paragraph 122 (and citations therein); Judgment of 27 February 1985 in *Société des produits de maïs*, C-112/83, EU:C:1985:86, paragraph 18.

prior to the date of the Court's judgment, except in respect of those workers who had already brought legal proceedings or made an equivalent claim.[105] In a similar way, the Court of Justice limited the temporal effect of its judgment in the *Barber* case.[106] In *Volker und Markus Scheke and Eifert*, the Court concluded that certain provisions of EU law permitting the publication of the personal data of beneficiaries under agricultural funds were invalid by reference to Articles 7 and 8 of the Charter but limited the consequences of its declaration of invalidity in view of the large number of publications which had already taken place in Member States.[107]

72. More recently, the Court of Justice has applied this reasoning by analogy to the situation of national courts addressing the consequences of declaring a provision of national law inconsistent with EU law in their domestic legal orders. While Member States are required to nullify the unlawful consequences of a breach of EU law, in exceptional cases, for overriding considerations of legal certainty, the Court may allow temporary suspension of the ousting effect of a rule of EU law with respect to contrary national law.[108] In Case C-41/11, the first *Inter-Environnement Wallonie* case, the Court noted that the referring court was not relying on economic grounds in order to maintain the effects of inconsistent national law but "*the objective of protecting the environment, which constitutes one of the essential objectives of the European Union and is both fundamental and cross-cutting in nature*".[109] In order to maintain the effects of inconsistent national law on a temporary and exceptional basis, the Court held that the following conditions must be satisfied: first, the contested national measure must be a measure transposing the relevant EU law; secondly, the adoption and coming into force of the new national measure must not make it possible to avoid the damaging effects arising from annulment; thirdly, the annulment of the national measure must have the effect of creating a legal vacuum; and, fourthly, the exceptional maintenance of effect of the contested national measure must last only so long as is strictly necessary for the adoption of measures remedying the irregularity found.[110] At the heart of this assessment lies the question of whether the overriding objectives of Union law would be better achieved by maintaining the effects of the inconsistent national law pending the adoption of amending measures.[111] The list of such objectives is not fixed. In Case C-411/17, the second *Inter-Environnement Wallonie* case, the Court of Justice was concerned with overriding considerations relating to the security of the electricity supply of the Member State concerned, in circumstances where there was a genuine and serious threat of disruption which could not be remedied by alternative means.[112] While it is for the Court of Justice to determine circumstances in which it may be justifiable, by way of exception, to maintain the effects of measures on account of such overriding considerations, it is for the national court to assess whether the conditions for doing so are satisfied in the particular case.[113]

---

[105] Judgment of 8 April 1976 in *Defrenne*, Case 43/75, EU:C:1976:56.
[106] Judgment of 17 May 1990, *Barber*, C-262/88, EU:C:1990:209, paragraphs 41-44.
[107] Judgment of the Court (Grand Chamber) of 9 November 2010, *Volker und Markus Schecke and Eifert*, Joined cases C-92/09 and C-93/09, EU:C:2010:662, paragraph 94.
[108] See judgment of 8 September 2010, *Winner Wetten*, C-409/06, EU:C:2010:503; judgment of 28 February 2012, *Inter-Environnement Wallonie*, C-41/11, EU:C:2012:103; judgment of 28 July 2016, *Association France Nature Environnement*, C-379/15, EU:C:2016:603, paragraph 33.
[109] *Inter-Environnement Wallonie*, EU:C:2012:103, paragraph 57.
[110] *Inter-Environnement Wallonie*, EU:C:2012:103, paragraphs 59-63.
[111] *Inter-Environnement Wallonie*, EU:C:2012:103, paragraph 55.
[112] Judgment of 29 July 2019, *Inter-Environnement Wallonie*, C-411/17, EU:C:2019:622, paragraph 179.
[113] *Inter-Environnement Wallonie*, EU:C:2019:622, paragraphs 179-180.

73. Indeed, in the pending reference in Case C-520/18, *Ordre des barreaux*, the Belgian Constitutional Court has raised this very issue in the context of its national data retention legislation. In his Opinion of 15 January 2020, Advocate General Campos Sánchez-Bordona has advised that the national court should be allowed to maintain national measures inconsistent with EU law, on an exceptional and temporary basis, on the basis of overriding considerations relating to threats to public or national security which cannot be averted by other means or alternatives.[114] According to the Advocate General, the objective of establishing an area of security in Article 3 TEU is no less transversal and fundamental than the objective of protecting the environment at issue in earlier cases.[115]

Application to the Present Case

74. For the reasons set out above, it is submitted that the first to fourth questions do not disclose any inconsistency with EU law. However, in the event that the national court were to conclude otherwise, it is submitted that there are overriding considerations of legal certainty and public interest of a compelling nature, which require that the effect of any declaration of inconsistency be suspended until the Irish Parliament has had an opportunity to remedy such inconsistency as may be found to exist in respect of the 2011 Act. In this regard, it is important to have regard to the following considerations.

75. First, at all stages up until 8 April 2014, Ireland was obliged as a matter of EU law to have in place a data retention regime of the kind enshrined in the 2011 Act. In the Plaintiff's case, all requests for access to retained data took place prior to 8 April 2014 and, thus, at a time when the State was obliged as a matter of EU law to have national data retention legislation in place. It would run contrary to the principle of legal certainty if a Member State could simultaneously be under an obligation under EU law to take certain measures while also, in taking such measures, be condemned for acting in breach of EU law. In its case-law, the Court has recognised the overriding considerations of legal certainty that arise where Member States rely in good faith on the legality of a particular provision or interpretation of EU law. In this case, those considerations of legal certainty are not merely abstract: the 2011 Act was enacted after an unsuccessful challenge to the validity of the Data Retention Directive and subsequent infringement proceedings against the Irish State. In these exceptional circumstances, it would be unjust to grant a declaration of inconsistency without any limitation on its temporal effect.

76. Secondly, while in *Digital Rights Ireland* this Court did not limit the effects of its declaration of invalidity,[116] that decision must be understood in light of the fact that the Data Retention Directive, which depended entirely on national implementing measures for its effect, did not have an independent life within national legal orders. Different considerations clearly apply in respect of national implementing measures which intervened in sensitive and complex areas of national law, affecting the day-to-day

---

[114] *Ordre des barreaux,* EU:C:2020:7, paragraphs 144-154.

[115] *Ordre des barreaux,* EU:C:2020:7, paragraph 150.

[116] In this regard, the Court did not follow the Opinion of the Advocate General who had proposed that it would be appropriate "*to suspend the effects of the finding that Directive 2006/24 is invalid pending adoption by the European Union legislature of the measures necessary to remedy the invalidity found to exist*", Opinion of Advocate General of Cruz Villalón of 12 December 2013, EU:C:2013:845, paragraph 158.

operation of law enforcement and national security, and which, in many cases, may have addressed the deficiencies identified by the Court in the Directive, particularly insofar as access was concerned.

77. Thirdly, in the period since *Digital Rights Ireland*, notwithstanding the many references which have been made to the Court, there has remained very significant uncertainty about the criteria applicable to national data retention measures and indeed the extent to which such measures fall within the scope of EU law. Member States have had to act without the benefit of any detailed legislative framework at EU level. As the history of the references in this field demonstrates, even where amending legislation has been proposed or adopted in a Member State, its validity has often been called into question, particularly by reference to the judgment in *Tele2 Sverige/Watson*. In the meantime, significant doubt has been cast over the use of a vitally important investigative tool across all Member States.

78. Fourthly, if national data retention legislation such as the 2011 Act were to be declared invalid without any suspension of effect, this could give rise to "*chaos and damage to the public interest*" to use the language referenced in the fifth question. First, in this particular case, such a declaration would lend support to the Plaintiff's criminal appeal in which he seeks to argue that the evidence obtained under the 2011 Act should not have been admitted at his trial.[117] If this argument were successful, this could do a grave injustice to the victim in this case and her family. Secondly, and even more significantly, such a declaration could have more general and systemic consequences, potentially casting doubt over the very many criminal investigations and prosecutions in which reliance has been placed on data retained and accessed under the 2011 Act.[118] This position could not be reconciled with the notion of an "*area of freedom, security and justice*" and the objective of preventing and combating crime recognised in Article 3(2) TEU. In the Defendants' submission, the *"overriding considerations of legal certainty"* at play in this case are of an equal if not greater order of magnitude than those which have justified the limiting the effects of invalidity or inconsistency in earlier cases.

79. Fifthly, with respect to the specific conditions identified in this Court's judgments in *Inter-Environnement Wallonie*, the Defendants make the following observations:

    (i) First, having regard to the lack of a detailed legislative framework at EU level, this is not a case of straightforward transposition or non-transposition of EU law. The contested national measure, the 2011 Act, was enacted specifically in order to transpose the Data Retention Directive and, since its invalidation, constitutes a national data retention measure falling within the scope of Article 15(1) of the e-Privacy Directive.

    (ii) Secondly, while the nature of any remedial legislation would depend on the particular form and basis of inconsistency, if the 2011 Act were struck down without any limitation on the effect of inconsistency, new legislation could not address the legal uncertainty arising in past and ongoing criminal proceedings in which reliance has been placed on the 2011 Act and thus could not avoid the damaging effects arising from the striking down of the 2011 Act.

---

[117] Reference, paragraph 8.6 and Appendix II, paragraph 6; see also Supreme Court Judgment, paragraph 6.10.

[118] In this regard, it is important to recall that "*the question of admissibility of evidence in a criminal trial is a matter of national law*": see Reference, paragraph 8.6.

(iii) Thirdly, if the 2011 Act were declared inconsistent without any temporal limitation, this would have the effect of creating a legal vacuum which could imperil the effectiveness of the fight against serious crime and threats to public security.

(iv) Fourthly, the effect of the 2011 Act would only be maintained for so long as was strictly necessary for the adoption of measures remedying the irregularity found. In this regard, it is relevant to note that, as a matter of Irish constitutional law, the Supreme Court and the Court of Appeal has suspended the effect of declarations of unconstitutionality for limited periods of time in a limited number of cases.

While the assessment of these conditions is ultimately a matter for the national court, in the Defendants' submission, this is a compelling case in which the overriding objectives of Union law would unquestionably be better achieved by maintaining the effects of the 2011 Act, insofar as it may be found to be inconsistent with EU law, pending the adoption of appropriate amending measures.

80. For all these reasons, it is submitted that, in the event that the 2011 Act were found to be inconsistent with EU law, the national court would be entitled to limit the temporal effect of any such declaration, including by suspending its effect pending the adoption within a reasonable but limited period of time of appropriate amending measures in order to bring national law in line with EU law.

IV. Conclusion

81. For these reasons, the Defendants submit that the Court should respond as follows to the questions referred:

> **With respect to the first and fourth questions**, a general data retention regime is not *per se* contrary to Article 15(1) of Directive 2002/58/EC, interpreted in light of the Charter. Neither Article 15(1) nor the Charter precludes the adoption or maintenance in force of national measures establishing a general data retention regime where it is established, on the basis of all available evidence, that such a regime is both essential and strictly necessary to the achievement of the objective of combating serious crime.
>
> **With respect to the second question**, in assessing the validity of a national data retention regime, a national court is entitled to have regard to the fact that data may be retained lawfully by service providers for their own commercial purposes, and may also be required to be retained for reasons of national security.
>
> **With respect to the third question**, a body may be regarded as an independent administrative body within the meaning of *Tele2 Sverige/Watson* where it is operationally and functionally independent and free of political or executive influence in the exercise of its function of carrying out prior review of access requests. In carrying out this assessment, a national court may have regard to mechanisms for *post factum* review.
>
> Without prejudice to the Defendants' answers to the first to fourth questions:
>
> **With respect to the fifth and sixth questions**, in the event that a national measure were declared to be inconsistent with EU law, a national court would be entitled to limit the temporal effect of any such declaration, including by suspending its effect pending the adoption within a reasonable but limited period of time of appropriate amending measures in order to bring national law in line with EU law.

Dated 7th August 2020

Signed: [redacted]
Sabina Purcell
Agent for Ireland
On behalf of Maria Browne, Chief State Solicitor

Signed: [redacted]
Tony Joyce
Agent for Ireland
On behalf of Maria Browne, Chief State Solicitor

Signed: [redacted]
Caroline Stone
Agent for Ireland
On behalf of Maria Browne, Chief State Solicitor