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

In **Joined Cases C-511/18 and C-512/18**

FRENCH DATA NETWORK, LA QUADRATURE DU NET, FÉDÉRATION DES FOURNISSEURS D'ACCÈS À INTERNET ASSOCIATIFS & IGWAN.NET

Applicants

-and-

PREMIER MINISTRE, GARDE DES SCEAUX, MINISTRE DE LA JUSTICE MINISTRE DE L'INTÉRIEUR & MINISTRE DES ARMÉES

Defendants

AND

FRENCH DATA NETWORK, LA QUADRATURE DU NET & FÉDÉRATION DES FOURNISSEURS D'ACCÈS À INTERNET ASSOCIATIFS

Applicants

-and-

PREMIER MINISTRE & GARDE DES SCEAUX, MINISTRE DE LA JUSTICE

Defendants

WRITTEN OBSERVATIONS OF IRELAND

Ireland, 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 David Fennelly BL of the Bar of Ireland, has the honour to submit written observations in these proceedings, the subject of joined references for preliminary ruling from the Conseil d'État (France) lodged on 3 August 2018.

Dated: 12 December 2018

I. Introduction

1. Ireland submits these Written Observations pursuant to Article 23 of the Protocol on the Statute of the Court of Justice of the European Union.

2. In Case C-511/18, the Conseil d'État (France) ("**the referring court**") has referred the following questions for preliminary ruling pursuant to Article 267 TFEU ("**Case C-511/18**"):

> 1. Is the general and indiscriminate retention obligation imposed on providers on the basis of the permissive provisions of Article 15(1) of the Directive of 12 July 2002 to be regarded, against a background of serious and persistent threats to national security, and in particular the terrorist threat, as interference justified by the right to security guaranteed in Article 6 of the Charter of Fundamental Rights of the European Union and the requirements of national security, responsibility for which falls to the Member States alone pursuant to Article 4 of the Treaty on European Union?
>
> 2. Is the Directive of 12 July 2002, read in the light of the Charter of Fundamental Rights of the European Union, to be interpreted as authorising legislative measures, such as the real-time measures for the collection of the traffic and location data of specified individuals, which, whilst affecting the rights and obligations of the providers of an electronic communications service, do not however require them to comply with a specific obligation to retain their data?
>
> 3. Is the Directive of 12 July 2002, read in the light of the Charter of Fundamental Rights of the European Union, to be interpreted as making the legality of the procedures for the collection of connection data subject in all cases to a requirement that the persons concerned are duly informed once such information is no longer liable to jeopardise the investigations being undertaken by the competent authorities, or may such procedures be regarded as lawful taking into account all the other existing procedural guarantees, since those guarantees ensure that the right to a remedy is effective?

3. In Case C-512/18, the Conseil d'État has referred the following questions for preliminary ruling pursuant to Article 267 TFEU ("**Case C-512/18**"):

> 1. Is the general and indiscriminate retention obligation imposed on providers on the basis of the permissive provisions of Article 15(1) of the Directive of 12 July 2002 to be regarded, *inter alia* in the light of the guarantees and checks to which the collection and use of such connection data are then subject, as interference justified by the right to security guaranteed in Article 6 of the Charter of Fundamental Rights of the European Union and the requirements of national security, responsibility for

which falls to the Member States alone pursuant to Article 4 of the Treaty on European Union?

2. Are the provisions of the Directive of 8 June 2000, read in the light of Articles 6, 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, to be interpreted as allowing a State to introduce national legislation requiring the persons whose activity consists in offering access to online public communications services and the natural or legal persons who, even free of charge, and for provision to the public via online public communications services, store signals, writing, images, sounds or messages of any kind provided by recipients of those services to retain the data capable of enabling the identification of anyone who has contributed to the creation of the content or some of the content of the services which they provide, so that the judicial authority may, where appropriate, require the communication of those data with a view to ensuring compliance with the rules on civil and criminal liability?

4. Thus, in the first question common to the References, the referring court asks in essence whether national legislation imposing on telecommunications service providers a general obligation to obtain traffic and location data is precluded by EU law having regard, in particular, to Article 4(2) TEU which provides that responsibility for national security falls to the Member States alone. In its observations, Ireland will focus on this first question.

5. In light of the fact that certain of the measures at issue in the domestic proceedings are national security measures, Ireland considers it necessary to address, as a preliminary matter, the scope of EU law. However, to the extent that the Reference falls within the scope of EU law, Ireland submits that EU law cannot be interpreted as precluding national legislation imposing on telecommunications service providers a general obligation to obtain traffic and location data.

II. The First Question Common to the Joined References

A. Retention for National Security Purposes Falls Outside the Scope of EU Law

6. These References, like the pending references in Case C-623/17, *Privacy International* and Case C-520/18, *Ordre des barreaux francophones et germanophone & Others*, present a fundamental question about the proper scope of EU law and, in particular, the extent to which EU law – in this case, Directive 2002/58/EC ("**the e-Privacy Directive**") – applies to Member

State activities in the field of national security. In particular, the measures at issue in the domestic proceedings in Case C-511/18 clearly lie within the field of national security and the measures at issue in Case C-512/18 may also extend to, and be used for the purposes of, national security.

7. In its Reference in Case C-511/18, in light of this Court's judgment in *Tele2 Sverige/Watson*, the referring court has stated that provisions laying down obligations on telecommunications service providers for the purposes stated in Article 15(1) of Directive 2002/58/EC *"fall within the scope of that directive since, as the Court of Justice has held, they regulate their activity"*. The referring court has also stated that *"national legislation providing for access to and use of such data likewise falls within the scope of [the Directive]"*. However, the referring court observed that, by contrast, *"national provisions concerning intelligence gathering techniques directly implemented by the State without regulating the activities of the providers of electronic communications services by requiring them to comply with specific obligations are not covered by the [Directive]"*.[1]

8. It is indeed the case that, in its judgment in *Tele2 Sverige/Watson*,[2] this Court – having referred to Articles 1(3) and 15 of the Directive – concluded that legislative measures referred in Article 15(1) were not *"excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose"*.[3] The Court continued:

> Indeed, Article 15(1) necessarily presupposes that the national measures referred to therein, such as those relating to the retention of data for the purpose of combating crime, fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met.[4]

The Court observed that the measures in question in those proceedings governed the activity of providers of electronic communications services.[5] The Court thus concluded that the

[1] Reference, Case C-511/18, paragraph 18.
[2] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970.
[3] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 73.
[4] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 74.
[5] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 74.

particular national data retention and access measures – at issue in *Tele2 Sverige/Watson* – fell within the scope of the Directive.[6]

9. In its recent judgment in *Ministerio Fiscal*, this Court concluded that Spanish measures regulating data retention for the purposes of fighting crime, because they *"necessarily"* involved the processing by providers of personal data, could not, to the extent that those measures regulated the activities of such service providers, *"be regarded as activities characteristic of States, referred to in Article 1(3) of Directive 2002/58"*.[7] According to the Court, the activities there mentioned are *"activities of the State or of State authorities and are unrelated to fields in which individuals are active"*.[8] Accordingly, the fact that the request for access to retained data by the relevant Spanish authorities was made in connection with a criminal investigation did not make Directive 2002/58 *"inapplicable to the case in the main proceedings by virtue of Article 1(3) of the directive"*.[9]

10. It is important to note that these judgments were both delivered in the context of national measures providing for the retention of, and access to, telecommunications data for the purpose of fighting crime, which, until the judgment in *Digital Rights Ireland & Others*,[10] had been the subject of regulation at EU level in the form of the Data Retention Directive. By contrast, there has not been – and, without an amendment of the Treaties conferring competence on the Union in this field, there could not be – any regulation of data retention for national security purposes at the EU level. In Ireland's submission, there is an important distinction between the competence of the EU in the field of data retention for the purpose of fighting crime, on the one hand, and for other purposes, in particular national security purposes, on the other hand. The expansive interpretation of Article 15(1), at the expense of Article 1(3), in these judgments should not be extended beyond the field of criminal law.

11. However, if and insofar the interpretation of Article 1(3) and Article 15 of the Directive in *Tele2 Sverige/Watson* and *Ministerio Fiscal* must be taken to apply also to retention for

---

[6] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 78.
[7] Judgment of 2 October 2018 in *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paragraph 37.
[8] Judgment of 2 October 2018 in *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paragraph 32.
[9] Judgment of 2 October 2018 in *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paragraph 39.
[10] Judgment of 8 April 2014 in *Digital Rights Ireland & Others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238.

national security purposes, it is respectfully submitted that this interpretation must be revisited for the following reasons.

12. Article 1(3) serves a fundamental role within the scheme of the Directive in defining its scope. It provides in the clearest of terms that the Directive *"shall not apply"* to activities falling outside the scope of the Treaties 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".* As Ireland has submitted in its observations in Case C-623/17 and Case C-520/18, properly understood, Article 1(3) is not a derogation or an exception which falls to be interpreted strictly. It does not render EU law *"inapplicable"* in excluded fields such as national security.[11] Rather, it provides that the relevant EU rules *simply do not in the first instance apply*. In the case of national security, the reason for this is obvious. In perhaps the most important and explicit marker of the division of competences between the Union and Member States in the Treaties, Article 4(2) TEU provides that "*national security remains the sole responsibility of each Member State".* In line with Article 4(2) TEU, the Union does not enjoy competence to legislate in the field of national security, whether in the context of data retention or otherwise. The EU legislature could not, on the basis of Article 95 EC or otherwise, regulate data retention in the field of national security.

13. It is not sufficient in this regard to consider whether national legislation regulates the activities of service providers without also having regard to the very nature and purpose of the activities are regulated under particular national legislation. Similarly, even if national security measures may involve non-State entities such as service providers, this does not deprive such measures of their character as *"activities of the State or of State authorities and are unrelated to fields in which individuals are active".*

14. In its judgment in Joined Cases C-317/04 and C-318/04, *Parliament v. Council & Commission*, the Court concluded that, although PNR was data initially collected by air carriers in the context of their commercial activities, the transfer of PNR data to US authorities under US national security legislation constituted *"processing operations*

[11] See, by way of contrast, Judgment of 4 June 2013, *ZZ*, C-300/11, ECLI:EU:C:2013:363, paragraph 38.

concerning public security and the activities of the State in areas of criminal law".[12] The Court continued:

> While the view may rightly be taken that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community law, namely sale of an aeroplane ticket which provides entitlement to a supply of services, the data processing which is taken into account in the decision on adequacy is, however, quite different in nature. As pointed out in paragraph 55 of the present judgment, that decision concerns not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes.
>
> The Court held in paragraph 43 of *Lindqvist*, which was relied upon by the Commission in its defence, that the activities mentioned by way of example in the first indent of Article 3(2) of the Directive are, in any event, activities of the State or of State authorities and unrelated to the fields of activity of individuals. However, this does not mean that, because the PNR data have been collected by private operators for commercial purposes and it is they who arrange for their transfer to a third country, the transfer in question is not covered by that provision. The transfer falls within a framework established by the public authorities that relates to public security.[13]

For this reason, by reference to Article 3(2), which is the analogue to Article 1(3) of the e-Privacy Directive, the Court concluded that the impugned adequacy decision fell outside the scope of Directive 95/46/EC and thus outside the scope of EU law.

15. Unfortunately, neither the judgment in *Tele2 Sverige/Watson* nor that in *Ministerio Fiscal* engages with this judgment. However, in Ireland's submission, the logic of the Court's reasoning in Cases C-317/04 and C-318/04 applies with equal force to the Member States' national security measures, such as the legislation at issue in Case C-511/04. Such an interpretation of Article 1(3) of the e-Privacy Directive – consistent with that of Article 3(2) of the Data Protection Directive in Cases C-317/04 and C-318/04 – is the only interpretation consistent with the legal basis for the e-Privacy Directive and the division of competences between the Union and Member States enshrined in Article 4(2) TEU.

16. Such an interpretation does not mean that Article 15(1) of the e-Privacy Directive is deprived of its purpose. As Ireland has previously submitted, Article 15(1) is a provision which seeks

[12] Judgment of 30 May 2006, *Parliament v. Council & Commission*, Joined Cases C-317/04 and C-318/04, ECLI:EU:C:2005:190, paragraph 56.
[13] Judgment of 30 May 2006, *Parliament v. Council & Commission*, Joined Cases C-317/04 and C-318/04, ECLI:EU:C:2005:190, paragraphs 57-58.

to address the co-existence of Union and Member State competence in a particular field and, to the extent possible, to ensure consistency between the two but it does *not* – and, in light of Article 4(2) TEU, it could *not* – bring within the scope of Union law the very matters which are excluded from the scope of the Directive and reserved to the Member States. If Article 15(1) were interpreted as bringing within the scope of the Directive, and thus EU law, matters which are explicitly excluded from its application and which lie outside Union competence, that provision would be incompatible not only with Article 95 EC, the legal basis on which the Directive was adopted,[14] but also, and more fundamentally, with Article 4(2) TEU. This would run contrary to the fundamental principle of conferral enshrined in Articles 4 and 5 on which the competence of the Union, and by extension the jurisdiction of this Court, is based.

17. In this regard, it is also important to have regard to the far-reaching implications of any finding by this Court that national security measures, such as those at issue in Case C-511/18, fall within the scope of EU law. Having regard to the very clear limits on the EU's competence to legislate in this field enshrined in Article 4(2) TEU, such measures would be considered to come within the scope of EU law without the EU legislature being in a position to adopt measures effectively regulating the field. Measures of this kind – which touch upon the most important and sensitive responsibilities of the Member States – cannot be effectively regulated by reference to a provision such as Article 15(1) of the e-Privacy Directive and the principles laid down in the jurisprudence of this Court alone. A clear and detailed legislative framework is vitally important to ensure that such measures comply with fundamental rights.

18. For these reasons, in Ireland's submission, to the extent that national legislation governing data retention regulates retention for national security purposes, such legislation does not fall within the scope of EU law.

B. EU Law Does Not Preclude National Legislation Imposing a General Retention Obligation

19. However, to the extent that the domestic measures at issue in these proceedings fall within the scope of EU law, it is submitted that neither Article 15(1) of the Directive, nor any other provision of EU law, precludes the adoption by Member States of national legislation which

[14] Judgment of 30 May 2006, *Parliament v. Council & Commission*, C-317/04 and C-318/04, ECLI:EU:C:2006:346.

lays down a general obligation for telecommunications service providers to retain traffic and location data for specified purposes, falling within the scope of EU law, and subject to appropriate safeguards.

20. In *Digital Rights Ireland*, this Court accepted that retained telecommunications data were a *"valuable tool for criminal investigations"*.[15] The Court concluded that general data retention – of the kind provided for in the Data Retention Directive – was *appropriate* for attaining the objective of fighting serious crime:

> As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive.[16]

The Court recognized that the fight against serious crime, in particular organized crime and terrorism, was *"indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques"*.[17] At the same time, the Court considered that such an objective of general interest did not *of itself* justify a retention measure such as that established by the Data Retention Directive being considered to be *"necessary for the purpose of that fight"*.[18] Ultimately, of course, 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, because of the Directive's failure to lay down clear and precise rules governing its scope and application and to impose minimum safeguards.[19] However, in reaching this conclusion by reference to the specific regime laid down in the Data Retention Directive which left the question of access to retained data entirely to Member States, the Court did not call into

---

[15] Judgment of 8 April 2014 in *Digital Rights Ireland & Others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 49.
[16] Judgment of 8 April 2014 in *Digital Rights Ireland & Others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 49.
[17] Judgment of 8 April 2014 in *Digital Rights Ireland & Others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 51.
[18] Judgment of 8 April 2014 in *Digital Rights Ireland & Others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 51.
[19] Judgment of 8 April 2014 in *Digital Rights Ireland & Others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraphs 54-69.

question its earlier conclusion that data retention, general in scope, was an appropriate means of achieving the objective of fighting serious crime.

21. In its judgment in *Tele2 Sverige/Watson*, this Court did, however, conclude 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"*.[20] At the same time, the Court observed that Article 15(1) *"does 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"*.[21] The Court then identified the salient features of such a regime:

    a. First, such legislation must *"lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards"*, in particular, indicating *"in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted"*;[22]

    b. Secondly, while the substantive conditions to be satisfied may vary according to the nature of the measures taken for the purposes of fighting serious crime, *"the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued"*, in particular by circumscribing, in practice, the extent of that measure and, thus, the public affected;[23]

    c. Thirdly, such 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*

[20] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970.
[21] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 108.
[22] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 109.
[23] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 110.

> *security"*. According to the Court, 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"*.[24]

22. While the Court stipulated that any data retention measures must be based on objective evidence,[25] it does not appear that there was any evidence before this Court in *Tele2 Sverige/Watson,* and there is no evidence before the Court in the present case, which would support the conclusion that *"targeted retention"* is either an appropriate means of achieving the objective of fighting serious crime or an effective alternative to general retention. While the Opinion of Advocate General Saugmandsgaard Øe in *Tele2 Sverige/Watson* made reference to a number of studies which questioned the necessity of general retention,[26] 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[27] or simply highlight the issues identified by this Court with the particular data retention regime established under the Data Retention Directive.[28]

23. Indeed such evidence as there is before the Court supports the conclusion that, in order to be an effective tool for these purposes, data retention must necessarily be general at the stage of retention. As the referring court has concluded in Case C-512/18, the usefulness of such a retention practice – i.e. general retention – is *"unparalleled with a view to investigating, establishing and prosecuting criminal offences"*.[29] Similarly, in Case C-511/18, the referring court has stated:

---

[24] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 111.
[25] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 111.
[26] Opinion of 19 July 2016 of Advocate General Saugmandsgaard Øe in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:572, paragraph 209, footnote 65.
[27] Council of Europe Commissioner for Human Rights, *Issue Paper on the rule of law on the Internet and in the wider digital world*, December 2014, CommDH/IssuePaper(2014)1, p. 115.
[28] Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age of 30 June 2014, A/HRC/27/37; Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism of 23 September 2014, A/69/397.
[29] Reference in Case C-512/18, paragraph 9.

> First, it is established that such preventative and indiscriminate retention allows the intelligence services to access data relating to the communications that an individual has made before the reasons for believing that he presents a threat to public security, defence or State security are identified. Against a background of serious and persistent threats to national security, and in particular the terrorist threat, the usefulness of such a retention practice is unparalleled as compared with the collection of those same data solely from the point at which the individual in question has been identified as liable to pose a threat to public security, defence or State security.[30]

This is also Ireland's experience. Such data play a vital role not only in the fight against serious crime but also in safeguarding national security. Indeed, in light of the significant rise in cybercrime, telecommunications data are of increasing importance and, in many cases, indispensable for the effective investigation and prosecution of serious offences. Similarly, in the context of evolving threats to national security, including terrorism, recourse to such data is ever more important. However, data retention can only be an effective tool for these purposes if it is general in scope at the stage of retention.

24. In an important recent judgment on the validity of the Irish data retention legislation, in the case of *Graham Dwyer v. Commissioner of An Garda Síochána & Others*, the High Court of Ireland was called upon to consider these issues in the light of the Court's judgment in *Tele2 Sverige/Watson*.[31] Mr Dwyer, an architect by profession, had engaged in a secret sexual relationship with Ms Elaine O'Hara over a number of years, using "master" and "slave" phones to communicate with each other. In August 2012, Ms O'Hara, who was a vulnerable individual with a history of mental health difficulties, went missing and her disappearance was initially treated as a missing persons case. In September 2013, when water levels were particularly low after a dry summer, a number of items were recovered from a reservoir outside Dublin, including certain belongings of Ms O'Hara and the "master" and "slave" phones. Around the same time, Ms O'Hara's body was found by a dog walker in the Dublin mountains. It was only through the use of location data from the discarded mobile phones that the police were eventually able to identify Mr Dwyer as a suspect. Once he was identified as a suspect, location data confirmed that the "master" phone was generally in use at or around the same location as Mr Dwyer's work phone. Such evidence was gathered at a time – prior to 8 April 2014 – when Ireland was bound, as a matter of EU law, to have such a general

[30] Reference in Case C-511/18, paragraph 24.

[31] *Graham Dwyer v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Ireland and the Attorney General* [2018] IEHC 685, available on the website of the Irish Courts Service (www.courts.ie).

retention regime in place. At trial, the judge rejected a challenge to the admissibility of the telecommunications data evidence on the basis that it had been obtained in breach of Mr Dwyer's rights. This evidence thus played a critical role in the investigation into Ms O'Hara's murder and ultimately in the successful prosecution of Mr Dwyer for the murder of Ms O'Hara. In early 2015, Mr Dwyer was convicted of murder of Elaine O'Hara and sentenced to life imprisonment. Mr Dwyer has appealed his conviction and, in a separate constitutional challenge, he has challenged the validity of the Irish data retention regime.

25. In the course of the hearing of this constitutional challenge, the High Court heard uncontroverted expert evidence that there are no effective alternatives to a general data retention regime.[32] In its judgment, the Court emphasized that the plaintiff in those proceedings had not established that the actual operation of the legislation from the date of retention to the date of disclosure was *"inappropriate, unnecessary or disproportionate"*.[33] Indeed, if the Irish legislation at issue had not required the general retention of traffic and location data, an effective investigation into the identity of the user of the "master" phone – and, with it, Ms O'Hara's murder – would have been seriously compromised.

26. Nevertheless, notwithstanding the evidence before it, the Court considered itself bound to conclude, by reason of this Court's judgment in *Tele2 Sverige/Watson*, that the general obligation to retain data imposed under the Irish legislation was inconsistent with EU law and that it could not even undertake a proportionality assessment of the domestic legislative regime in this regard.[34] The Court also concluded that the legislation was inconsistent with EU law insofar as it failed to provide for any prior review by a court or independent administrative authority of access to retained telephony data and to provide adequate legislative guarantees against abuse.[35] Mr Dwyer will now seek to rely on this judgment in his pending criminal appeal. The judgment also has very significant potential implications for other criminal investigations and prosecutions.

---

[32] *Graham Dwyer v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Ireland and the Attorney General* [2018] IEHC 685, paragraphs 2.23-2.25.
[33] *Graham Dwyer v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Ireland and the Attorney General* [2018] IEHC 685, paragraph 5.17.
[34] *Graham Dwyer v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Ireland and the Attorney General* [2018] IEHC 685, paragraphs 3.63-3.65.
[35] *Graham Dwyer v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Ireland and the Attorney General* [2018] IEHC 685, paragraphs 3.106.

27. While this case is merely one example of the invaluable role of retained communications data in the investigation of the most serious of crimes, the *Dwyer* case illustrates in a vivid way, by reference to the facts of a real and concrete case and on the basis of expert evidence, why retention must be general, rather than targeted, at the initial stage of retention in order to be an effective law enforcement and security tool.

28. Furthermore, the *Dwyer* case – and in particular the Court's conclusion that, in light of *Tele2 Sverige/Watson*, it was not even possible to undertake a proportionality assessment of the validity of a general retention regime (despite the uncontroverted evidence before it that this was the only effective form of retention) – illustrates the fundamental difficulty, from an evidential point of view, with the Court's position in *Tele2 Sverige/Watson* that EU law precludes a general, but not a targeted, obligation to retain telecommunications data.

29. It must be emphasized that the real and distinctive value added of data retention – as opposed to other possible tools such as data preservation[36] – is that it can assist in identifying persons who were hitherto unknown to the authorities in the context of investigations into serious crime and national security. In providing the authorities with access, subject to appropriate safeguards, to historical telecommunications data, data retention can also allow evidence trails to be established, including on the movements of suspects, victims or witnesses to serious crime and those involved in threats to national security, such as terrorism. In many cases, without access to this data, investigations would be fundamentally undermined. In particular, the investigation and prosecution of many serious forms of cybercrime, such as online child sexual exploitation and child pornography, would be severely compromised without access to retained telecommunications data.[37]

30. That real and distinctive value would be lost if Member States could only make provision for some form of *"targeted retention"* of the kind referred to in *Tele2 Sverige/Watson*, which appears to share the limitations of data preservation. In particular, in investigating serious

[36] Data preservation was rejected by the EU legislature as an effective alternative to data retention both prior to the adoption of the now invalidated Data Retention Directive and in 2011 in the context of its evaluation: see 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, 1, 5-6, 13; European Commission, *Evaluation report on the Data Retention Directive*, COM(2011) 225, pp. 1 and 5.

[37] See e.g. David Anderson, *A Question of Trust: Report of the Investigatory Powers Review*, June 2015, paragraphs 7.47, 14.19-22.

crime and in safeguarding national security, such a tool would be wholly ineffective for the purpose of identifying suspects or persons of interest – such as Mr Dwyer – who are otherwise unknown to the authorities. In Ireland's submission, a system of targeted retention – which would be prospective only in its application and defined by reference to characteristics such as geographical or other criteria which apparently tend to show a link with serious crime[38] – would be unworkable and ineffective in practice.

31. Moreover, a *"targeted retention"* regime of this kind would also be very difficult to justify in principle. Such a regime – which would operate by targeting or profiling, for example, persons living in a particular geographical zone or defined by reference to other relevant characteristics – could not itself be reconciled with the fundamental rights and freedoms protected under the Charter of Fundamental Rights, in particular the guarantee of non-discrimination enshrined in Article 21. While such a regime might involve a less serious degree of interference with the fundamental rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter, it would at the same time be difficult to reconcile with other fundamental rights and values of the Union.

32. In this regard, it is important to have regard to the important role that data retention measures may play in the prevention, detection, investigation and prosecution of serious crimes and terrorist attacks which constitute a direct attack on the right to security of person enshrined in Article 6, the relevance of which was recognized by this Court at paragraph 42 of its judgment in *Digital Rights Ireland*. In addition, data retention measures may play an important role in ensuring that Member States respect the positive obligations arising under provisions such as Article 2 of the Charter (for example, for murder victims such as Ms O'Hara), Article 4 and Article 7 of the Charter.[39]

33. Moreover, while national security is, in accordance with Article 4(2) TEU, a fundamental responsibility of Member States, which lies outside the scope of the Union's competence, as discussed above, in considering whether EU law precludes a general retention obligation for

---

[38] Mr. Justice John L. Murray, *Review of the Law on Retention of and Access to Communications Data*, Department of Justice and Equality of Ireland, April 2017, paragraphs 242-245, available online at http://www.justice.ie/en/JELR/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf/Files/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf (last accessed 4 December 2018).

[39] See by analogy the judgment of 2 December 2008, European Court of Human Rights, *K.U. v. Finland*, CE:ECHR:2008:1202JUD000287202.

matters falling within its scope, this Court must have regard to the fact that Member States consider such a general retention obligation to be essential for the safeguarding of national security.

34. In circumstances where data retention is only effective and valuable as a law enforcement and national security instrument if it is generalized in scope at the retention stage, Ireland submits that it cannot be concluded that a general data retention regime is *per se* disproportionate or contrary to the Charter.

***

35. For these reasons, it is submitted that Article 15(1) of the Directive does not preclude the adoption by Member States of national legislation which lays down a general obligation for telecommunications service providers to retain traffic and location data for specified purposes and subject to appropriate safeguards.

III. The Second and Third Questions in Reference C-511/18

36. Turning to the second question in Reference C-511/18, the referring court asks whether the e-Privacy Directive, read in light of the Charter, is to be interpreted as authorising legislative measures, such as the real-time measures for the collection of the traffic and location data of specified individuals, which, whilst affecting the rights and obligations of the providers of an electronic communications service, do not however require them to comply with a specific obligation to retain their data.

37. By its third question, the referring court asks if the e-Privacy Directive, read in light of the Charter, is to be interpreted as making the legality of the procedures for the collection of connection data subject in all cases to a requirement that the persons concerned are duly informed once such information is no longer liable to jeopardise the investigations being undertaken by the competent authorities, or may such procedures be regarded as lawful taking into account all the other existing procedural guarantees, since those guarantees ensure that the right to a remedy is effective.

38. Strictly without prejudice to its submission that the national measures at issue in Reference C-511/18 fall outside the scope of EU law, Ireland makes the following observations on this second question.

39. By way of preliminary observation, it is submitted that these questions illustrate the difficulty faced by Member States where a complex and sensitive policy issue is deemed to fall within the scope of EU law without there being any detailed and effective legislative framework in place at EU level.

40. On the substance of the second question, Ireland submits that, having regard to the terms of Article 15(1) of the e-Privacy Directive, that provision must be interpreted as authorizing such legislative measures. The first sentence of that provision is framed in general terms, recognizing that Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for under other provisions of the Directive for specified purposes and subject to certain conditions. The second sentence of that provision provides that, to this end, Member States may *inter alia* adopt data retention measures. It is thus clear that the legislative measures which Member States may adopt are not limited to data retention measures and may include real-time measures for the collection of the traffic and location data of specified individuals which do not involve the retention of data.[40]

41. On the substance of the third question, Ireland notes that, in *Tele2 Sverige/Watson*, this Court concluded – in the context of national data retention measures in the field of criminal law – that competent national authorities which access retained data *"must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities"*.[41] According to the Court, such notification *"is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive*

[40] See Judgment of 8 February 2018, European Court of Human Rights (Fifth Section), *Ben Faiza v. France*, Application No. 31446/12. The Court observed at paragraph 74 :"À cet égard, la Cour considère qu'il est pertinent de distinguer les méthodes d'investigations permettant de géolocaliser une personne a posteriori de celles qui permettent de la géolocaliser en temps réel, ces dernières étant davantage susceptibles de porter atteinte au droit d'une personne au respect de sa vie privée. En effet, la communication de la liste des cellules déclenchées par une ligne téléphonique permet certes de connaître, a posteriori, le positionnement géographique passé de l'utilisateur de cette ligne. Mais il s'agit de la transmission à l'autorité judiciaire de données existantes et conservées par un organisme public ou privé et non de la mise en place d'un dispositif de surveillance, consistant à repérer spécifiquement les déplacements qu'une personne est en train de réaliser, par le biais d'un suivi dynamique d'une ligne téléphonique ou au moyen de la pose d'une balise sur un véhicule".

[41] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 121.

2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed".

42. Thus, in principle, EU law must be interpreted as requiring persons concerned to be notified once the information in question is no longer liable to jeopardise the investigations being undertaken by the competent authorities. However, as the purpose of such notification is to enable the exercise of the right to a legal remedy in cases of infringement, Ireland submits that, if there are other effective procedural guarantees which ensure the protection of the right to an effective remedy in this context, an absolute requirement of notification may not strictly be necessary.

IV. The Second Question in Reference C-512/18

43. By its second question in Reference C-512/18, the referring court asks if the provisions of Directive 2000/31/EC, the e-Commerce Directive, read in light of the Charter, are to be interpreted as allowing a State to introduce national legislation requiring the persons whose activity consists in offering access to online public communications services and the natural or legal persons who, even free of charge, and for provision to the public via online public communications services, store signals, writing, images, sounds or messages of any kind provided by recipients of those services to retain the data capable of enabling the identification of anyone who has contributed to the creation of the content or some of the content of the services which they provide, so that the judicial authority may, where appropriate, require the communication of those data with a view to ensuring compliance with the rules on civil and criminal liability.

44. It would appear that the legislative measure at issue – namely, paragraph II of Article 6 of the *Loi du 21 juin 2004* – imposes an obligation on persons who offer access to online public communications services and those persons who, in connection with such services, store data, to retain data capable of identifying persons involved in the creation of the content of such online public communication services and, further, that access to such data is subject to prior judicial review. Such a retention obligation is therefore limited in scope, relates to content on online *public* communications services, serves a legitimate objective, and would appear to be subject to appropriate safeguards.

45. Such legislation does not constitute *"a general obligation to monitor information ….[or] actively to seek facts or circumstances indicating illegal activity"* contrary to Article 15(1) of Directive 2000/31/EC. Instead it would appear to fall within the scope of the permissive provision of Article 15(2) of the Directive which allows Member States to "*establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements*". Thus, in Ireland's submission, Directive 2000/31/EC, interpreted in light of the Charter, in principle allows a Member State to adopt legislation of the kind at issue in the domestic proceedings.

V. Conclusion

46. FOR THESE REASONS, it is submitted that the Court should respond as follows to the Joined References:

With respect to the first question common to both References, to the extent that such measures fall within the scope of EU law, neither Article 15(1) of Directive 2002/58/EC nor any other provision of EU law precludes measures imposing a general obligation to retain data for specified purposes and subject to appropriate safeguards.

With respect to the second question in Case C-511/18, Directive 2002/58/EC, read in light of the Charter of Fundamental Rights, must be interpreted as authorising legislative measures, such as the real-time measures for the collection of the traffic and location data of specified individuals, which, whilst affecting the rights and obligations of the providers of an electronic communications service, do not however require them to comply with a specific obligation to retain their data.

With respect to the third question in Case C-511/18, Directive 2002/58/EC, read in light of the Charter of Fundamental Rights, is not to be interpreted as imposing an absolute requirement to notify a person the subject of data retention and access measures once such information is no longer liable to jeopardise investigations undertaken by the competent authorities if there are other effective procedural guarantees which ensure the protection of the right to an effective remedy.

With respect to second question in Case C-512/18, Directive 2000/31/EC, read in light of the Charter of Fundamental Rights, in principle allows a Member State from

adopting legislation imposing an obligation on persons who offer access to online public communications services and those persons who, in connection with such services, store data, to retain data capable of identifying persons involved in the creation of the content of such online public communication services.

Dated 12 December 2018

Signed: Gemma Hodge
Agent for Ireland
on behalf of Maria Browne, Chief State Solicitor

Signed: Tony Joyce
Agent for Ireland
on behalf of Maria Browne, Chief State Solicitor