

**IN THE COURT OF JUSTICE OF THE EUROPEAN UNION**

**JOINED CASES C-511/18 and C-512/18**

**FRENCH DATA NETWORK  
LA QUADRATURE DU NET  
& others**

---

**WRITTEN OBSERVATIONS OF THE UNITED KINGDOM**

---

The United Kingdom is represented by Simon Brandon of the Government Legal Department, acting as Agent, and by Gerry Facenna QC and Christopher Knight, Barristers.

Submitted by:

Simon Brandon  
Agent for the United Kingdom  
Government Legal Department  
Room 3/01  
1 Horse Guards Road  
London  
SW1A 2HQ

Gerry Facenna QC  
Christopher Knight  
  
Barristers

Service may be made by e-curia or email  
Email: [simon.brandon@dex.eu.gov.uk](mailto:simon.brandon@dex.eu.gov.uk)

**7 December 2018**

## INTRODUCTION & SUMMARY

1. Pursuant to Article 23 of the Protocol on the Statute of the Court of Justice of the European Union, the United Kingdom submits the following written observations on the questions referred for a preliminary ruling under Article 267 of the Treaty on the Functioning of the European Union (“TFEU”) by the Conseil d’État (“the Referring Court”) in its Orders lodged on 3 August 2018 (“the Orders for Reference”).
2. The Referring Court’s questions on both Orders for Reference concern the compulsory retention of connection and online data by electronic communications operators and technical service providers, so as to enable subsequent access to that data by appropriate security and intelligence agencies (“SIAs”) or a judicial authority. Further, the Referring Court asks in C-511/18 whether the right to an effective remedy requires the notification to the individual data subject of access to connection data.
3. In summary, the United Kingdom submits as follows:
  - (1) Competence for Member States’ national security lies exclusively with the Member States. It is not a competence which has been conferred by the Treaties on the EU. On the contrary, Article 4(2) TEU clearly and expressly identifies national security as being the sole responsibility of Member States.
  - (2) Real-time access to connection data for the specific purpose of protecting national security does not fall within the scope of EU law.
  - (3) Any interference with rights for the purposes of investigating serious crime, and which falls within the scope of EU law, would be proportionate and lawful.
  - (4) Notification of access to retained connection data is not a pre-condition to legality of national law, in order to establish the existence of an

effective remedy. The European Court of Human Rights correctly recognises the need to conduct a holistic and contextual assessment.

(5) Directive 2000/31/EC contains no prohibition on national law requiring the retention of information society services data, which is instead regulated by data protection law read with the Charter.

4. Further, the United Kingdom suggests that there is sufficient and significant overlap between the issues arising in the Orders for Reference and those arising in Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs*, that these present references should only be determined following the judgment of this Court in Case C-623/17.

#### **PRELIMINARY OBSERVATIONS ON THE USE OF COMMUNICATIONS DATA**

5. By way of context, the United Kingdom recalls the critical public interest in SIAs across the Union being able to access telecommunications data when it is needed for purposes that include the fight against terrorism. See, for further details, the Order for Reference in Case C-623/17 *Privacy International*.
6. Communications service providers collect a great deal of data through commercial interactions with their customers. Such data includes, for example, personal and financial information about the customer, as well as data on the time and duration of communications. Such data is legitimately used by service providers for commercial purposes, for example to accurately bill their customers.
7. In the context of the national law in issue in C-511/18, the retained communications data consists of the subscription numbers of the specified person, the mapping of all associated numbers, the location of the terminal equipment, the list of numbers called and calling, and the duration and date of the communications. The national law in issue does not concern the *content* of any communication: rather, it is connection data. Access to such data, including real-time access in specified circumstances, is restricted to national SIAs

investigating and preventing threats to national security, and in particular, terrorism.

8. In the context of the national law in issue in C-512/18, the data retained is that which enables the identification of a person using an electronic communications service who has created or contributed to the creation of content online, subject to a maximum retention period of one year. Access to such identifying data is limited to judicial authorities, for the investigation, detection and prosecution of criminal offences, intellectual property infringements and attacks on the data processing systems themselves. The national law does not concern retention of online content, but rather communications data enabling identification of the user.
9. Communications data can be of vital importance, including for investigations into terrorism, threats to public security and organised crime. In March 2013 the Commission published a report drawing together evidence from the Member States as to the necessity for data retention within the EU.<sup>1</sup> Section 8 of that report, entitled 'Qualitative Data', contains information about a large number of real cases across the EU in which communications data were crucial, in preventing or investigating serious crime or terrorism. A similar analysis is to be found in a report of the United Kingdom's former Independent Reviewer of Terrorism Legislation<sup>2</sup> and its Intelligence and Security Committee of Parliament.<sup>3</sup> It is clear that a number of Member States face an acute threat

---

<sup>1</sup> *Evidence for necessity of data retention in the EU*, March 2013, available at

<sup>2</sup> David Anderson QC (now Lord Anderson QC), 'A Question of Trust' (June 2015), especially at chapter 9, available at <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf>.

<sup>3</sup> Intelligence and Security Committee of Parliament, 'Privacy and Security: A Modern and Transparent Legal Framework' (2015), especially at chapter 6, available at [https://b1cba9b3-a-5e6631fd-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312\\_ISC\\_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7crOE2HRdQ4O8IfYwWWZqRmTsENvEswZo4wsLNNNA930od19nGNU95AjBP6TCSMMbQuh23bOoyxPQttWt7DyKLWawWJtO9spMZs-OgZouWfZGefokQ1P1HtqmFYyR4B40CRuD3B8AwDJ0cl-eLeu1aJRvjogqv63JKjGLkz6A5irrWclMxrXdxhEgbv6ycZi\\_7gLj-G9A6kP7-BOSagtSHB0cMcjbxl9C5EXPdO1-pqOc\\_T3yR\\_VC0nwq3HO\\_QZsrxWwJlkth&attredirects=0](https://b1cba9b3-a-5e6631fd-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7crOE2HRdQ4O8IfYwWWZqRmTsENvEswZo4wsLNNNA930od19nGNU95AjBP6TCSMMbQuh23bOoyxPQttWt7DyKLWawWJtO9spMZs-OgZouWfZGefokQ1P1HtqmFYyR4B40CRuD3B8AwDJ0cl-eLeu1aJRvjogqv63JKjGLkz6A5irrWclMxrXdxhEgbv6ycZi_7gLj-G9A6kP7-BOSagtSHB0cMcjbxl9C5EXPdO1-pqOc_T3yR_VC0nwq3HO_QZsrxWwJlkth&attredirects=0)

from terrorism, as repeated and appalling recent attacks across Europe indicate.<sup>4</sup>

10. Without the ability to use and analyse communications data, including analysing activity online, the critical work of the Member States' SIA and law enforcement authorities in combating crime and fighting terrorism would be severely weakened.
11. The Court has previously recognised that the fight against crime, in particular against organised crime and terrorism, is a legitimate objective of the utmost importance, in order to ensure public security. The Court has also acknowledged that the effectiveness of that fight may depend to a great extent on the use of modern investigation techniques, including the use of communications data, which is an essential tool in that fight.<sup>5</sup>
12. It follows that the Court should avoid imposing overly restrictive conditions on the ability of the Member States to determine that a criminal activity or threat to public security is sufficiently 'serious' to justify law enforcement agencies making use of communications data, subject to oversight by national judicial authorities.

## **OBSERVATIONS ON QUESTION 1 IN BOTH ORDERS FOR REFERENCE**

13. The Referring Court asks in Question 1 of both Orders for Reference, whether the retention of communications data is a matter which falls to the Member States alone, in accordance with Article 4 of the Treaty on European Union ("TEU").
14. The United Kingdom recognises that the national laws in issue in the Orders for Reference appear to have different focuses. The legislation in Case C-511/18 is focussed on the activities of the SIAs and the protection of national security.

---

<sup>4</sup> For example, Europol publishes statistics of the number of failed, foiled or completed terrorist attacks in the EU. In 2016 there were 142 of these recorded, with more than half (76) recorded in the UK. See <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2018/01/Terrorism-Acts-in-2016.pdf> at paragraph 2.4.

<sup>5</sup> C-293/12 and C-594/12 *Digital Rights Ireland* (EU:C:2014:238), paragraphs 41-44, 49, 51.

The legislation in Case C-512/18 is focussed principally around wider criminal law enforcement. The former is a matter wholly outside the scope of EU law. The latter is a matter principally for the Member States, who are well-placed to address such matters, in the light of relevant national circumstances.

15. Article 5 TEU limits Union competences by reference to the principle of conferral. Article 4(1) TEU makes clear that competences not conferred on the Union remain with the Member States. These Treaty provisions are ‘jurisdictional’ in nature. They set out the scope – and limits – of EU law. They are not dealing with the manner in which conferred competence is exercised, but with whether competence has been conferred at all.
16. Article 4(2) TEU makes clear that safeguarding national security is an essential State function. It emphasises explicitly that “*national security remains the sole responsibility of each Member State*” (emphasis added). Similarly, “*maintaining law and order*” is recognised as an essential function of the Member States rather than the EU, as is the need to respect “*the different legal systems and traditions of the Member States*” in the area of freedom, security and justice: see Article 67(1) Treaty on the Functioning of the European Union (“TFEU”). The TFEU confirms that responsibility for national security and policing remains with Member States, and is not conferred upon the EU: see Articles 73 and 276.
17. This is unsurprising. Member States are particularly well placed to assess both the nature of the threats faced and the means by which they can be combated.<sup>6</sup> EU law does not impose on Member States a uniform scale of values as regards the assessment of conduct which may be considered to be contrary to public security: Case C-348/09 *PI* (ECLI:EU:C:2012:300), paragraph 21.<sup>7</sup> Threats to a State’s national security represent a direct challenge to its ability to perform its essential state function of the protection of its people, its territorial integrity and its sovereignty. Such threats are varied and unpredictable in their

---

<sup>6</sup> See, e.g., Case C-83/94 *Leifer* [1995] ECR I-3231, paragraph 35; Case C-367/89 *Richardt* [1991] I-4621, paragraph 22.

<sup>7</sup> See also: Joined Cases 115 and 116/81 *Adoni* [1982] ECR 1665, paragraph 8; Case C-268/99 *Jany* [2001] ECR I-8615, paragraph 60.

nature, their extent and their source. Threats can emanate from hostile States, organised groups of insurrectionists and terrorists, or physically unconnected individuals inspired by a shared ideology of violence. Threats can emerge unannounced and change at speed. Illustrative (but non-exhaustive) examples may be terrorism and sabotage, actions intended to overthrow or undermine parliamentary democracy, cyber-attacks affecting public services, border incursions, espionage, or the development by stealth of nuclear, biological or chemical weapon capability or intention. The nature and level of threats, and therefore the nature of an appropriate measure to illuminate and respond to such threats, may also vary considerably between States. The way in which Member States seek to pre-empt these threats and stay ahead of them will vary and touches on some of the most essential and sovereign aspects of a State's responsibility.

18. In the related area of criminal law enforcement, the substantive content of criminal law and the rules of criminal procedure are matters for which Member States are alone responsible.<sup>8</sup> Member States retain exclusive competence as regards the maintenance of public order and the safeguarding of national security, and they enjoy a margin of discretion in combatting criminality.<sup>9</sup> This approach is consistent with the wide margin of discretion afforded to Contracting States in the adoption of particular criminal justice measures by the European Court of Human Rights.<sup>10</sup>
19. In the context of provisions dealing with jurisdiction or competence, the choice is between competence being conferred on the EU by Member States, being shared between the EU and Member States or being retained by Member States and not conferred on the EU. The use of the word “*sole*” is very clear in Article 4(2) TEU: responsibility for national security lies with the Member States, not the EU. It is not a competence conferred upon the EU in the Treaties. There is a contrast between national security matters – which are entirely excluded –

---

<sup>8</sup> Case 203/80 *Casati* [1981] ECR 2595, paragraph 27.

<sup>9</sup> Case C-265/95 *Commission v France* [1997] ECR I-6959, paragraph 33; Case C-394/97 *Criminal Proceedings against Heinonen* [1999] ECR I-3599, paragraph 43.

<sup>10</sup> *Vinter v United Kingdom* (2016) 63 EHRR 1, paragraphs 104-105.

and criminal law enforcement, as to which Article 4(2) recognises that the EU shares some competence, but that Member States retain primacy.

20. Article 4(2) is not a derogation from EU law. It is a foundational Treaty provision falling to be interpreted as such. That is confirmed by the International Law Decision of 18-19 February 2016 at section C.5:

*“Article 4(2) of the Treaty on European Union confirms that national security remains the sole responsibility of each Member State. This does not constitute a derogation from Union law and should therefore not be interpreted restrictively. In exercising their powers, the Union institutions will fully respect the national security responsibility of the Member States.”*<sup>11</sup>

21. The effect of Article 4(2) was considered in Case C-51/15 *Remondis* (ECLI:EU:C:2016:985). That case concerned the issue of whether the definition of “*public contracts*” in the EU directive on public procurement extended to an agreement between two regional authorities to form a common special-purpose association with separate legal personality. The CJEU answered it by reference to Article 4(2) TEU, adopting the view of Advocate-General Mengozzi in his Opinion (ECLI:EU:C:2016:504) that such matters fell outside the scope of EU law altogether. It is apparent that:

- (1) The matters covered by Article 4(2) are solely matters for each Member State and do not fall under EU law. The fact that the Union must respect “*essential State functions*” (including the division of responsibility as between national, regional and local government, and, in the present case, national security) is consistent with the principle of conferral of powers laid down in Articles 5(1) and (2) TEU, no provision having conferred on the Union the power to intervene in such matters: see the Opinion of AG Mengozzi at paragraphs 38-39.

---

<sup>11</sup> On 18-19 February 2016, the Heads of State or Government of the 28 Member States of the European Union, meeting within the European Council, made a Decision concerning a new settlement for the United Kingdom within the European Union. The Decision did not formally come into force given that the United Kingdom did not vote to remain a member of the European Union in the referendum. However, in accordance with Article 31 of the Vienna Convention on the Law of the Treaties, it remains an interpretative decision agreed by all parties to the EU Treaties.

(2) As acts of secondary legislation such as a directive must be in conformity with primary law (i.e. the Treaties), they cannot be interpreted as permitting interference in matters to which Article 4(2) TEU applies. Such matters remain outside the scope of EU law and, more specifically, EU rules set out in a directive: see the Opinion of AG Mengozzi at paragraphs 41-42, as endorsed by the CJEU in its Judgment at paragraphs 40-41. National security (and, to some extent, criminal law) is quintessentially such a matter, as emphasised not only by the second sentence of Article 4(2) TEU but also the third sentence.

22. Directive 2002/58/EC translates the established principles of Directive 95/46/EC<sup>12</sup> into specific rules in relation to electronic communications services. Article 1(3) of Directive 2002/58/EC effectively replicates the terms of Article 3(2) of Directive 95/46/EC and provides that it:

*“shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, 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.”*<sup>13</sup>

23. It is thus plain that the EU legislature correctly recognised the limited scope of the Directive, limited by reference to the competence of the EU itself. In light of the primacy of Article 4(2) TEU, that was inevitable and was a necessary recognition in the case of essential State functions relating to national security and criminal law enforcement. Competence in national security matters has consciously not been conferred upon the EU at all, but retained as the sole responsibility of Member States. The degree to which the EU is entitled to scrutinise criminal law enforcement is limited. It would be constitutionally impermissible for a Directive to make provision to the contrary. Article 1(3) of Directive 2002/58/EC accordingly excludes such matters from its scope.

---

<sup>12</sup> See: Article 3(2) of that Directive and Case C-101/01 *Lindqvist* (ECLI:EU:C:2003:596) at paragraph 43 and Case C-73/07 *Satakunnan Markkinapörssi* (ECLI:EU:C:2008:727) at paragraph 41.

<sup>13</sup> See also recital (11) of Directive 2002/58/EC.

24. Article 15(1) of Directive 2002/58/EC includes reference to “*national security*”. However, that cannot be taken to override Article 1(3), and still less Article 4(2) TEU, given the primacy of the Treaties. It makes provision for the avoidance of doubt, as it also does for the entire scope of the criminal law (not limited by reference to ‘serious crime’). The effect of Article 4(2) TEU, reflected properly in Article 1(3), is to create an exemption from the scope of EU law and of the Directive in particular – not to provide for a derogation. As already noted, it would be constitutionally impermissible for a provision in a Directive to purport to create competence where none exists under the TEU. Thus, the inclusion of such wording in Article 15(1), in the context of a provision which otherwise appears to refer to grounds for derogation, is incapable of bringing within scope of the Directive matters of Member State responsibility which are intended to be excluded from the scope of EU law altogether. Nor can Article 1(3) be deprived of purpose by Article 15(1).
25. To this extent, the United Kingdom considers that the Referring Court has wrongly framed the first question in both Orders for Reference as arising from the terms of Article 15 of Directive 2002/58/EC, instead of the terms of Article 4(2) TEU, to which it correctly refers at the end of the first question.
26. Neither Case C-203/15 *Tele2 Sverige* (ECLI:EU:C:2016:970) nor Case C-207/16 *Ministerio Fiscal* (ECLI:EU:C:2018:78) concerned the retention of, or access to, communications data specifically in the national security context. The distinction drawn and applied in those cases – see, e.g., paragraphs 29-39 of *Ministerio Fiscal* – has no or no material relevance in, at least, Case C-511/18. While the national law in issue in Case C-512/18 appears more closely to fall within the terms of the reasoning in *Tele2* and in *Ministerio Fiscal*, the Court must approach any application of EU law (including the Charter) to areas of criminal law enforcement with a degree of care, commensurate with the terms of Article 4(2) and the Court’s limited jurisdiction in this area.
27. The core issue of characterisation – whether the activity is properly characterised as within national security and the terms of Article 4(2) TEU –

cannot be answered by reference to any peripheral, or adventitious, involvement of a communications provider, so as to seek to use that involvement in effect to open up competence not merely in relation to transmission, but also in relation to all the subsequent activities of SIAs. It would cut across a faithful application of the clear division of competences in Article 4(2), in circumstances where the activities in question are all plainly national security activities and the vast majority of them have nothing whatever to do with service provision by commercial providers.

28. Indeed, the Grand Chamber of this Court has already held that the transfer of personal data collected by private operators for commercial purposes to State authorities pursuant to national legislative requirement adopted in the interests of public security and the activities of the state in areas of criminal law, does not fall within the scope of EU law. That approach was correct, and faithful to Article 4(2)'s intention. It so held in Joined Cases C-317/04 and C-318/04 *Parliament v Council* (ECLI:EU:C:2006:346), paragraph 59, when it decided that Commission Decision 2004/496, that adequate arrangements had been made for the protection of bulk PNR data (collected for airlines' commercial purposes) transferred to the United States authorities, fell outside the scope of the Data Protection Directive. The reason was that the processing of such data "*falls within a framework established by the public authorities that relates to public security*": see paragraph 58. *A fortiori*, processing of data involved in activities such as involved in these cases cannot fall within the scope of Directive 2002/58. Following the Lisbon Treaty, Article 4(2) TEU put this beyond doubt.
29. Moreover, it must be recalled that regardless of the scope of EU law, any activity of a Member State concerning the retention of, and access to, communications data will be a matter subject to the scrutiny of the European Court of Human Rights for compliance with the ECHR and, in particular, Article 8 ECHR. The Strasbourg Court recognises and accepts that Member States must be permitted a wide margin of appreciation in communications data contexts, but that there will nonetheless be scrutiny for compliance with essential safeguards: see, e.g., *Big Brother Watch v United Kingdom* (App. No. 58170/13) (judgment of 13 September 2018), paragraphs 314-315.

30. The United Kingdom therefore submits, in answer to the first question in both Orders for Reference, that a retention obligation imposed on providers in the context of serious and persistent threats to national security, and particularly the threat of terrorism, is a matter which falls within the competence of the Member States alone, and not the EU, in accordance with Article 4(2) TEU.

### **OBSERVATIONS ON QUESTION 2 IN CASE C-511/18**

31. The Referring Court asks whether Directive 2002/58 permits provisions of national law regulating access by SIAs to connection data for the purposes of prevention of terrorism, in circumstances where those access provisions do not require retention of data.
32. As the United Kingdom understands the context of this question, it concerns provisions of French law which permit SIAs real-time access to connection data being processed by communications providers in the context of a terrorist threat.
33. In this context, and regardless of the answer to the first question, the actions and processing concerned in the second question arise solely from the activities of the State, and in particular, the State's SIAs. These fall squarely within Article 4(2), including by reference to the distinction drawn in *Tele2 Sverige* and in *Ministerio Fiscal*. The impact on the providers of electronic communications services is limited to requiring them to permit real-time access to the SIAs in specific, limited, national security contexts. The distinction drawn by the Court between the governance of the activities of providers, and the direct activities of the State, as summarised in paragraphs 29-39 of *Ministerio Fiscal*, would be applicable here: it is the activities of the State which are regulated. It does not fall within the scope of Directive 2002/58 – or EU law – at all.
34. Further, even if such a measure were within the scope of EU law, it constitutes in principle a permissible exercise of the derogation in Article 15(1) of Directive 2002/58, the terms of which are not restricted to national measures providing for retention of communication data. Article 15(1) permits national laws to provide for exceptions to or derogations from the various rights and obligations set out

in the Directive, including apparent limitations on how and when different categories of communications data may be accessed.

35. Although an assessment of the proportionality of any national measure is a matter for the national court, the United Kingdom submits that the provisions of national law in issue under the second question of Case C-511/18 are so targeted and limited to the threat posed by terrorism and to action by the SIAs, that there can be no serious doubt that any degree of interference with Article 7 and/or 8 Charter rights is proportionate in the circumstances. This assessment is further strengthened by the recognition that the nature of any interference is to be viewed relative to the legitimate aim sought to be achieved by the interference – here the protection of the lives and safety of the public through the protection of national security – and having regard to the overall balance running through the Charter (just as through the ECHR) between private rights and freedoms and the general interests of the community.
36. The Court must recall that in the context of anti-terrorism, it is not only the rights of affected data subjects in issue. Articles 2 and 4 of the Charter recognise the fundamental rights to life and to live free from torture or inhuman and degrading treatment. The scales must not be thought empty when balancing the rights and degrees of interference in issue.
37. The United Kingdom submits that the answer to the second question is that Directive 2002/58/EC does not authorise a national legislative measure which permits security and intelligence agencies to access real-time connection data for the purposes of investigating and preventing terrorism, because that is a State activity which falls outside of the scope of EU law in accordance with Article 4(2) TEU and Article 1(3) of the Directive.
38. In the alternative, if Directive 2002/58 does apply, Article 15(1) does authorise such national measures and the relevant provisions of national law are proportionate to any limited interference with the Article 7 and/or 8 Charter rights of data subjects.

**OBSERVATIONS ON QUESTION 3 IN CASE C-511/18**

39. The Referring Court asks whether Directive 2002/58 requires in all cases a data subject to receive notification that his connection data has been collected, or whether other existing procedural guarantee of an effective remedy are sufficient.
40. The United Kingdom recalls that the Order for Reference in Case C-511/18 considers and rejects at paragraphs 7-14 a complaint that the provisions of national law failed to provide an effective remedy in breach of Article 13 ECHR. The Court should accordingly accept that appropriate and effective national legal mechanisms apply to the legal framework under challenge, which ensure that individuals are able to have tested in an effective manner any complaint of a breach of their fundamental rights to privacy.
41. Nothing in Directive 2002/58 itself imposes any requirement of notification. The Court in *Tele2 Sverige* at paragraph 121 articulated the need for notification of access to an individual's communications data on the basis of the effective exercise of their right to a legal remedy. This was itself based on the jurisprudence of the Strasbourg Court: *Tele2 Sverige* at paragraph 120.
42. However, the Court's observations in *Tele2 Sverige* on the issue of notification did not form part of the core reasoning of the Court, and are not mentioned in the *dispositif*. Secondly, the Court did not suggest in *Tele2 Sverige* that a requirement of notification of retention was a precondition to legality. Such a suggestion would be impractical. A general requirement to notify an individual that their data has been accessed would risk informing criminals, suspected criminals and others of investigative techniques that public authorities use. The fact that a particular investigation may have ceased, or that an individual is ruled out of a particular investigation, does not mean that notification would not be damaging to ongoing operations.
43. Thirdly, even in relation to access, the consistent approach of the European Court of Human Rights is that Convention rights are complied with as proportionate and providing an effective remedy where the Contracting State

provides for a route of challenge before an independent authority. A specific notification to the individual data subject of access to his personal data is not a pre-condition for legality or proportionality: *Kennedy v United Kingdom* (2011) 52 EHRR 4 at paragraph 167; *Centrum för Rättvisa v Sweden* (App. No. 35252/08) (judgment of 19 June 2018), paragraphs 171-178; *Big Brother Watch v United Kingdom* (App. No. 58170/13) (judgment of 13 September 2018), paragraphs 375-383. There is no reason nor necessity for the Court, particularly given Article 52(3) of the Charter, to depart from the Strasbourg Court's holistic and contextual approach.

44. Finally, in circumstances where the Referring Court has already found that the national legislation is consistent with the right to an effective remedy under Article 13 ECHR, the principled basis for notification has already been satisfied, whether under the ECHR or the Charter.
45. The United Kingdom submits that the answer to the third question referred in Case C-511/18 is that Directive 2002/58/EC does not require in all cases as a condition of legality a notification to the data subjects of access to connection data, where the national legislative scheme as a whole provides for an effective remedy.

## **OBSERVATIONS ON QUESTION 2 IN CASE C-512/18**

46. The Referring Court asks whether Directive 2000/31/EC permits Member States to require those offering access to online public communications services to retain the data capable of enabling the identification of anyone who has contributed to the content of the services which they provide, in order that that data may be provided upon authorised request to ensure compliance with the civil and criminal law.
47. Article 15(1) of Directive 2000/31 prohibits Member States from imposing any general obligation on an information society service provider to monitor the information transmitted to or stored by it, or actively to seek facts or circumstances indicating illegal activity; see also Case C-484/14 *McFadden*

(ECLI:EU:C:2016:689) at paragraph 87. However, Articles 14 and 15(2), and the case law of the Court, envisage that a provider may be retaining data concerning the use of the services it provides, which can be provided to third parties seeking to enforce legal rights: see, e.g., Case C-324/09 *L'Oréal SA* [2011] ECR I-6011 at paragraphs 110-111, 118-124. Whether any particular access or enforcement action is proportionate in any given case will involve the balancing of different applicable fundamental rights: *McFadden*, paragraphs 83-84.

48. The United Kingdom accordingly agrees with the observation of the Referring Court at paragraph 14 of the Order for Reference that Directive 2000/31 does not prohibit, or make subject to a specific form of derogation, the compulsory retention by an information society services provider of any particular form of data acquired through the provision of its services. Directive 2001/31 simply does not address such an issue.
49. Rather, any national legal measure which required the retention of data by information society service providers would be subject – in principle and subject to Article 4(2) TEU – to Directive 95/46/EC (and now Regulation 2016/679/EU), the Charter, and the case law of the Court, including *Tele2 Sverige*. In other words, retention of and subsequent access to data held by information society services providers which enables the identification of a user responsible for particular content, for the purposes of enforcement of the civil and criminal law, is permissible, but subject to the same legal controls as any other requirement to retain personal data.
50. The United Kingdom submits that the answer to the second question referred in Case C-512/18 is that Directive 2000/31/EC does not prohibit or control national law requiring the retention of and subsequent access to data held by information society services providers which enables the identification of a user responsible for particular content, for the purposes of enforcement of the civil and criminal law, but that such national law must be compatible with EU data protection law, including Charter rights.

**THE UNITED KINGDOM'S PROPOSED ANSWERS TO THE QUESTIONS**

51. The United Kingdom suggests the following answers to the questions posed by the Order for Reference in Case C-511/18:

*Question 1*

A retention obligation imposed on providers in the context of a serious and persistent threats to national security, and particularly the threat of terrorism, is a matter which falls within the competence of the Member States alone, and not the EU, in accordance with Article 4(2) TEU.

*Question 2*

Directive 2002/58/EC does not authorise a national legislative measure which permits security and intelligence agencies to access real-time connection data for the purposes of investigating and preventing terrorism, because that is a State activity which falls outside of the scope of EU law in accordance with Article 4(2) TEU and Article 1(3) of the Directive.

*Question 3*

Directive 2002/58/EC does not require in all cases as a condition of legality a notification to the data subjects of access to connection data, where the national legislative scheme as a whole provides for an effective remedy.

52. The United Kingdom suggests the following answers to the questions posed by the Order for Reference in Case C-512/18:

*Question 1*

A retention obligation imposed on providers in the context of a serious and persistent threats to national security, and particularly the threat of terrorism, is a matter which falls within the competence of the Member States alone, and not the EU, in accordance with Article 4(2) TEU.

*Question 2*

Directive 2000/31/EC does not prohibit or control national law requiring the retention of and subsequent access to data held by information society services providers which enables the identification of a user responsible for particular content, for the purposes of enforcement of the civil and criminal law, but such national law must be compatible with EU data protection law, including Charter rights.

Submitted by:



Simon Brandon  
Agent for the United Kingdom

Gerry Facenna QC  
Christopher Knight  
Barristers

**7 December 2018**