[TRANSLATION FROM THE FRENCH]

COURT OF JUSTICE OF THE EUROPEAN UNION

Case Nos. C-511/18 and C-512/18

regarding preliminary rulings of the Council of State (France)

between

French Data Network; La Quadrature du Net; Federation of Associated Internet Access Providers; Igwan.net

Petitioners

and

Privacy International; Center for Democracy and Technology

Intervening Parties

versus

Prime Minister; Keeper of the Seals, Minister of Justice; Minister of the Interior; Minister of the Armed Forces

Defendants

BRIEF FILED BY

PRIVACY INTERNATIONAL

Filed on 26 November 2018 by:

Hugo ROY | Attorney at Law
[…]

Table of Contents

1. The UK non-governmental, non-profit organization Privacy International (hereinafter "Intervener") intervened in February 2016 before the Council of State, along with the US non-governmental, non-profit organization Center for Democracy and Technology, in support of the request of French organizations requesting the annulment of the French Government's implicit refusal to repeal the regulatory provisions which result, in particular, from Decree No. 2006-358 of March 24, 2006 regarding the retention of communications data, adopted nine days after Directive 2006/24.[1] In so doing, Intervener intended to ensure the continuity of the Digital Rights judgment[2] handed down by the Court's Grand Chamber, which declared the aforementioned Directive 2006/24 as invalid.

2. The Intervener intends to argue in this brief that the grounds on which the Court's Grand Chamber ruled in the above-cited Digital Rights case, in the Schrems case[3], as well as in the Tele2/Watson case[4], shall apply in these joint cases, for the following reasons.

3. **Firstly**, it shall apply, by law, because of the absence of any significant change of circumstances since December 21, 2016 - the date of the Tele2/Watson judgment. The needs related to the fight against crime and the safeguarding of national security in the context of a real terrorist threat, are not new and have not changed scale since 21 December 2016.

4. Likewise, the applicable legal framework remains substantially identical with regard to the provisions of European Union law on which the Court's Grand Chamber has relied. Indeed, neither Directive 2002/58[5], nor the Charter of Fundamental Rights of the European Union (the "Charter") have been the subject to any amendment since December 2016. Even though European Union law on the protection of personal data has changed with the repeal of Directive 95/46[6]; the entry into force of Regulation 2016/679 (the "GDPR")[7] now ensures a consistent, high level of protection, and equivalent between its Member States. In particular, the right to seek effective remedy in the event of infringement to the personal data protection rights, as provided for in Article 22 of Directive 95/46, is now provided for in Article

[1] Directive 2006/24/EC of the European Parliament and Council dated March 15, 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services and public communications networks, amending Directive 2002/58/EC.
[2] CJEU, Grand Chamber, Apr. 8 2014, Digital Rights Ireland et al, C-293/12, C-594/12.
[3] CJEU, Grand Chamber, Oct. 6 2015, Schrems, C-362/14.
[4] CJEU, Grand Chamber, Dec. 21 2016, Tele2 Sverige, Watson et al., C-203/15, C-698/15.
[5] Directive 2002/58/EC of the European Parliament and Council dated July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications).
[6] Directive 95/46/EC of the European Parliament and the Council dated October 24, 1995 regarding the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[7] Regulation 2016/679 of the European Parliament and the Council dated April 27, 2016 regarding the protection of individuals with regard to the processing of personal data and the free movement of said data, repealing Directive 95/46/EC (General Data Protection Regulation).

79 of the GDPR. Finally, since May 2018, EU law has been applying the principle of "data minimization" both with the GDPR (Articles 5 (1) (c), 25 and 89 in particular) and with Directive 2016/680 8 (Articles 4 (1) (c) and 20)[8]. Overall, the level of protection of personal data required in the Union is higher today than in 2016.

5. **Secondly**, this interpretation is necessary to guarantee respect for fundamental rights and freedoms and, in particular, the right to privacy and the right to the protection of personal data. With regard to the development of the Internet and electronic communications services and the importance of their use in private and familial lives, in the exercise of the freedom of expression, as well as in the participation to democracy, the guarantees necessary to ensure the confidentiality of electronic communications must be considered as fundamental in a democratic society.

6. As attorney general Øe pointed out in his opinion in the joint cases Tele2 and Watson (C-203/15 and C-698/15) dated July 19, 2016, "the risks associated with access to communications data (or "metadata") may be equivalent to or even greater than those resulting from access to the content of such communications"; "the metadata" facilitate the almost instantaneous cataloguing of entire populations" (paragraph 259). As already noted by the Grand Chamber of the Court, "that data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them" (Tele2/Watson judgment, paragraph 99 and Digital Rights judgment, paragraph 27). It follows that a general and indiscriminate retention of all connection data [*Note of translation: this term under French law covers "traffic and location data" and "identification data" – excluding any content of electronic communications.]* constitutes a particularly serious and wide-ranging interference incompatible with the respect for the Charter (see, in particular, Tele2/Watson, paragraph 100 and Digital Rights, paragraph 37).

7. **Thirdly**, the opposite interpretation would open the possibility of national derogations which would neutralize or fragment the consistent, high level protection of personal data, equivalent in all the Member States, as well as weaken the full effect of the Charter. The opposite interpretation would therefore contribute to challenge area of freedom, security and justice without internal frontiers which the European Union granted to its citizens under Article 3 (2) of the European Union Treaty.

8. As will be shown, after a discussion of the relevant legal framework in the main proceedings for the purpose of providing the Court with details regarding the stakes of this case (Section 1), the retention of electronic communications data imposed on

[8] Directive 2016/680 of the European Parliament and of Council dated April 27, 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention and detection of criminal offenses, investigation and prosecution or the execution of criminal sanctions, and the free movement of such data, repealing Council Framework Decision 2008/977/JHA.

providers cannot be general and indiscriminate (Section 2 Page 9), and the collection of such data by authorities must be strictly regulated, as well as subject to a prior decision by a Court or an independent authority (Section 3, Page 13), and be accompanied by a notification to the affected data subjects as soon as the notification of this information is no longer likely to compromise the investigations conducted by these authorities (Section 4 Page 15).

1. CLARIFICATIONS REGARDING THE CHALLENGED LEGAL FRAMEWORK

9. As regards the first questions in Cases C-511/18 and C-512/18, the challenged legal framework is comparable to that of Tele2 Sverige (C-203/15) in that it raises the question of the implementation of Directive 2006/24.

10. The challenged legal framework was established in the wake of September 11, 2001 with the adoption of Law No. 2001-1062 of November 15, 2001 on everyday security. Since then, this frame work has been expanded and made more complex.

11. Without reviewing the challenged legal framework in its entirety, set forth in the contents of the referring judgment, Intervener wishes to make the following clarifications in order to inform the Court of the first questions raised by the joint cases, as well as the second and third questions related to Case No. C-511/18.

1.1 The data retention at issue is not limited to the fight against terrorism and its prevention

12. The national measures at issue in the main proceedings are in no way limited to the purposes of safeguarding national security. These measures are in pursuit of much broader goals. The retention of connection data under French law has been, in particular, used for purposes of preventing, establishing and prosecuting crimes and criminal offenses (not limited to serious crimes). Additionally, since 2001, French law has continuously expanded the possibilities of access to such retained data, for various purposes and activities. For example, Article L. 621-10 of the Monetary and Financial Code allows the communication of such data to investigators and auditors of the Financial Markets Authority.[9] Finally, the aims pursued for access to such data by the administrative authorities under Section VIII of the Internal Security Code relates to "the defense and promotion of the fundamental interests of the Nation" listed in Article L. 811-3 of the Internal Security Code, which include, in particular, the prevention of attacks to the public order,[10] the defense and promotion of

[9] This provision, considered unconstitutional, however, remained in force until December 31, 2018. See Council Const., 21 July 2017, Right to communication regarding AMF investigators login data, 2017-646/647 QPC.

[10] The text cites "collective violence likely to seriously undermine the public peace" in the meaning of Articles 431-1 to 431-10 of the Criminal Code and includes in particular the offense defined in Article 431-9 of the Penal Code which consists of "having organized a demonstration on the public road which has not been the object of “a prior declaration under the conditions set forth by law". Punishable by six months of imprisonment, it cannot be considered a serious crime (Conseil Constit., July 23, 2015, Intelligence Act, 2015-713 DC, considering 10).

France's major economic, industrial and scientific interests,[11] as well as the prevention of organized crime.[12]

1.2 The serious difficulty of interpretation raised by the challenged legal framework goes beyond the scope of the questions submitted

13. Regarding the second issue raised in Case C-511/18, the referring court cites "measures for the real-time collection of data relating to the traffic and location of specific individuals". Intervener submits that the referring court has excluded a significant part of the legal framework challenged in the main proceedings.

14. The question before the Court relates mainly to Article L. 851-2 of the Internal Security Code. This Article provides for a real-time collection of connection data, particularly by electronic communications networks, targeting certain persons in connection with a threat.[13]

15. Therefore, the referring court did not refer the Court with a question concerning Article L. 851-3 of the same Code. In Paragraph 1, this Article provides that "it may be imposed upon [electronic communications] operators [...] to implement automated processing on their networks, according to parameters specified in the authorization, to detect connections likely to reveal a terrorist threat ". This Article therefore provides for data processing: (i) real-time, (ii) using connection data (including personal data), (iii) on electronic communications networks inter alia. Article, L. 851-3, therefore has a purpose that is similar, and complementary, to that of Article L. 851-2. But Article L. 851-3 applies to a network and its entirety, and therefore all its users, without any limitation on the material scope or on the affected individuals.

16. Article L. 851-3 raises, as does Article L. 851-2, if not more so, a serious difficulty of interpretation as regards conformity with European Union law. However, the referring court decided not to submit to the Court any question on whether the implementation of such automated processing, directly on the provider's infrastructure, and in accordance with technical parameters determined by the State, is justified and limited to what is strictly necessary, as required by the Charter. This exclusion is all the more surprising since the Council of State's public rapporteur had rightly invited the referring court to include this article in the scope of its preliminary questions (see the Opinion of the Public Rapporteur, Page 13, Third and Fourth Paragraphs).[Exhibit No. A.1]).

---

[11] These interests are included in the fundamental interests of the nation within the meaning of Article 410-1 of the Criminal Code, according to the interpretation of the provisions of Article L. 811-3 of the Internal Security Code by the Council on Constitutional Law (ibid.)

[12] This purpose refers to the criminal indictments listed in Article 706-73 of the Code of Criminal Procedure and offenses punishable under Article 414 of the Customs Code committed by organized gangs (ibid.)

[13] "A person previously identified who may be in contact with a threat [or] one or more persons belonging to the entourage of the person concerned by the authorization [who] may provide information " (L. 851 -2, paragraph I.)

17. The Intervener emphasizes to the Court the opportunity to reiterate what the appropriate safeguards and the scope of those safeguards are, as regards data processing, which affects the confidentiality of electronic communications.

1.3 The procedural safeguards of the legal framework at issue are insufficient to compensate for the lack of notification of the affected persons

18. With regard to the third question raised by Case C-511/18, the referring court cites "existing procedural safeguards" around the collection of connection data. The Intervener therefore calls the Court's attention in particular to the following points.

19. **First**, there is no mechanism to effectively and sufficiently compensate for the absence of any ex-post notification. Articles L. 833-4 and L. 841-1 of the Internal Security Code provide that any person may refer to the National Commission for the Control of Intelligence Technology (CNCTR) or the Council of State for the purpose of "verifying that s/he has not been made the subject of an improper intelligence investigation ". However, this mechanism cannot be regarded as "an adequate possibility to request and obtain information about interceptions from the authorities" within the meaning of the case-law of the European Court of Human Rights (ECtHR, General Court, Dec. 4, 2015, Zakharov v. Russia, no 47143/06, § 298).

20. Indeed, at no time does the CNCTR provide significant information to the affected person. At best, pursuant to Articles L. 773-6 and L. 773-7 of the Code of Administrative Justice, the decision of the Council of State merely informs the claimant of the existence or non-existence of an unlawful action in the context of intelligence measures, without giving access to any relevant factual element for the exercise of the effective remedy of the claimant, nor any details on the data collected.

21. **Secondly**, in the context of ex-post proceedings, the secrecy for national security very often prevents an open hearing before the Council of State. Indeed, Article R. 773-24, Paragraph 1, of the Code of Administrative Justice provides that "[i]n cases where the proceedings are likely to involve information protected by the secrecy for national security, or to confirm or refute the implementation of an intelligence measure with regard to the claimant, or revealing elements contained in the data processing, or if the claimant has not been affected by the measure, the claimant is invited to withdraw before the statement of the opinion of the Public Rapporteur. [. . .]" This exclusion is all the more problematic as all public policies are considered to contribute to national security according to Article L. 1111-1, Paragraph 2, of the Defense Code. In addition, according to the Decree of November 30, 2011 approving General Inter-ministerial Instruction No. 1300 on the Protection of National Defense Secrecy, "the protection of secrecy concerns all fields of activity relating to defense and national security: political, military, diplomatic, scientific, economic, industrial."

22. Pursuant to Articles 413-9 of the French Criminal Code and R. 2311-6 of the French Defense Code, all elements which have been subject to a classification measure are deemed to be confidential on grounds of national defense, as decided by the

administrative and ministerial authorities themselves. Any declassification procedure, pursuant to Article L. 2312-4 of the Defense Code, must involve the Advisory Committee on National Defense Secrecy (CCSDN), but the administrative authorities are not bound by any opinions issued by it.

23. It follows that the public authority can itself, without effective and independent oversight, completely exclude certain information from an open hearing merely by placing it under the seal of secret for national security. Finally, and correspondingly, the provisions of Articles L. 773-1 to L. 773-8 of the Code of Administrative Justice infringe the right to an effective remedy by failing to provide a set of measures likely to effectively counterbalance the public authority's privileged access to a set of documents protected by the secret for national security.

24. **Thirdly**, in terms of international type of surveillance, the persons concerned have no right to remedy to the Council of State. International surveillance broadly covers "surveillance of communications that are issued or received abroad ". It is governed exclusively by a special legal regime (Articles L. 854-1 to L. 854-9 of the Internal Security Code). Therefore, access to a court is totally ineffective (for an illustration, see the case of European Parliament Member Sophie in't Veld (Council of State, Special Court, June 20, 2018, In't Veld, Nos. 404012 and 404013)).

25. As a result of the foregoing, according to Intervener, it is important to highlight the necessary guarantees without which processing of connection data carried out in the absence of consent of the data subjects and interfering with the confidentiality of communications, cannot be considered in compliance with European Union law, and in particular, compliance with the Charter.

2. FIRST QUESTIONS RAISED BY CASE Nos. C-511/18 AND C-512/18

26. The Court has been asked to determine whether the interference caused by a national measure providing for a general and indiscriminate retention, imposed on the providers of electronic communications services, may be regarded as justified, taking into account the Member States sole responsibility to safeguard national security. These first two questions thus implicitly refer to the Tele2/Watson judgment issued by the Grand Chamber. Although this judgment focuses on the fight against crime, its reasoning applies mutatis mutandis to the safeguarding of national security and in the context of real terrorist threats.

27. The Intervener observes, as a preliminary point, that the legal framework for the storage of connection data is far from meeting the requirements and guarantees handed down by the Grand Chamber in this respect (Tele2/Watson, Paragraphs 108 to 111). This obligation to retain data is not targeted with regard to the scope of data retained preventively. This obligation applies systematically, whatever the circumstances. All subscribers and users are therefore affected, directly, without distinction or objective limitation, as regards the objective pursued. Nor does the legal framework provide the guarantees necessary to protect against the risks of abuse.

28. The question raised relates specifically to the pursuit of objectives relating to the safeguarding of national security, taken in the context of a risk of terrorism (although the disputed framework is in no way limited to this, see Section 1.1 Page 5). However, neither the pursuit of these purposes, nor this context, allows for the measures at issue to be considered outside the scope of European Union law. These purposes and context do not call either for a different interpretation from that made by the Grand Chamber in the Tele2/Watson.

2.1. The Charter is fully applicable to the data processing at issue

29. The first questions state that safeguarding national security is the sole responsibility of the Member States. However, national laws affecting an activity subject to European Union law cannot be regarded as totally outside the scope of the said European Union law. Even if these national variances pursue purposes related to national security, they must be adequate, strictly limited to what is strictly, and proportionate.

30. The European Union has a strong legal framework for the regulation of the electronic communications sector, which governs the activities of electronic communications service providers and the use of these services. It is in this context that Directive 2002/58 was enacted, with the objective provided for in Article 1 "to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy " in this sector. Article 3 states that this Directive "applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Community". Directive 2002/58 must therefore be regarded as governing the activities of electronic communications service providers (Tele2/Watson judgment Paragraph 70).

31. The data retention obligations imposed on the providers referred to in the main proceedings, and to which the first questions relate, regard the activities of the providers of electronic communications services and hence the scope of Directive 2002/58 (see, by correlation, Tele2/Watson judgment, Paragraph 75). As the Court has already pointed out, this scope also applies to measures taken on grounds of national security, as cited in Article 15 Section 1 (paragraphs 71 to 73).

32. If limitations on the rights and obligations provided for by European Union law are permitted for the pursuit of objectives relating, in particular, to the safeguarding of national security (see, for example, Article 15 above, or Article 23 of the GDPR); it is under the conditions that such limitations are adequate, strictly necessary and proportionate, in the meaning of the Charter.

33. In fact, the applicability of EU law requires that of the Charter (CJEU, Grand Chamber, Feb. 26, 2013, Åklagaren, C-617/10, Paragraph 21). Consequently, there can be no case which falls within the scope of European Union law, without the

fundamental rights guaranteed by the Charter also being applied. Therefore, the Charter applies even in situations that involve matters of national security.

34. By consequence, EU law, and in particular Article 15 (1) of Directive 2002/58 as read in the light of the Charter, is fully applicable to the data retention requirements imposed on providers such as the national measures in the main proceedings.

2.2 The general and indiscriminate nature of data retention is incompatible with a democratic society

35. The interference, caused by a general and indiscriminate data retention requirement, with the fundamental rights enshrined in Articles 7 and 8 of the Charter is far-reaching and must be regarded as particularly serious (see, inter alia, Tele2 / Watson, Paragraph 100 and Digital Rights judgment, Paragraph 37).

36. In view of the gravity of this interference, only sufficiently serious purposes may be invoked in support of said interference, in accordance with the Charter, such as a serious crime (Tele2/Watson, Paragraph 102). The safeguarding of national security, taken in the context of real terrorist threats and in connection with the fight against them, can undeniably be considered as such. Intervener, however, invites that the Court follow a restrictive interpretation of the scope of the concept of safeguarding national security, in accordance with international law. The European Court of Human Rights considers that the scope of this concept should not be left to the total discretion of States (see, for example, Zakharov, Paragraph 248).

37. Nevertheless, as the Grand Chamber already ruled in December 2016, although the effectiveness of the fight against terrorism may depend to a large extent on the use of modern investigative techniques, such a general objective, however fundamental, cannot alone justify national regulations providing for the general and indiscriminate retention of all traffic and location data as necessary for the purposes of that fight (Tele2/Watson, Paragraph 103 and, by correlation, Directive 2006/24, Digital Rights judgment, Paragraph 51). It is not sufficient for such a legal measure to be considered appropriate in light of the objectives being pursued, in order to comply with Article 15 Paragraph 1, pursuant to the Charter. It is indeed required that it is also limited to what is strictly necessary and, ultimately, proportionate.

38. A general and indiscriminate data retention requirement covers all subscribers and users in general, without any differentiation, limitation or exception depending on the objective pursued. It globally concerns all people making use of electronic communications services. With regard to the development of the Internet and electronic communications services and the importance of their use in the private and family life, in the exercise of freedom of expression, as well as in participation in democratic life, such a measure affects almost the entire population of the Member State concerned. It is even applicable to persons for whom there is no evidence to legitimately suggest any connection with the objectives of safeguarding national security or a terrorist threat (see, by correlation, Tele2/Watson judgment, Paragraph

105 and, in the case concerning Directive 2006/24, Digital Rights judgment, Paragraph 57).

39. Except by considering that anyone is suspected of being a potential threat to the security of the State - a state of generalized suspicion incompatible with a democratic society - a general and indiscriminate data retention requirement, by its very nature, exceeds the limits of what is strictly necessary.

40. In that regard, in the Zakharov judgment cited above, the Grand Chamber of the European Court of Human Rights held that this requirement is also necessary in matters of national security and that the competent authority for the authorization of the interception "must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security." (Paragraph 260).

41. Moreover, such a requirement provides no exception for persons subject to professional secrecy (see, by correlation, Tele2/Watson, Paragraph 105 and, in the case of Directive 2006/24, Digital Rights judgment, Paragraph 58).

42. For all these reasons, general and indiscriminate data retention requirements cannot therefore be considered as being limited to what is strictly necessary, and are therefore contrary to the requirements of the Charter.

3. SECOND QUESTION IN CASE NO. C-511/18

43. The Court has been asked to determine whether the interference caused by a national regulation providing for real-time collection of data related to traffic and location of specific individuals, and affecting the rights and obligations of electronic communications service providers, may be regarded as justified even though it does not impose a specific requirement upon them to retain data.

44. As a preliminary point, the Intervener states that not all of the national measures at issue in the main proceedings which concern data which the providers of electronic communications services are obliged to retain, and which are provided for the sole purpose of prevention of terrorism, are targeting specific individuals (see Section 1.2 Page 6). The Intervener invites that the Court take into consideration the complementary nature of the measures at issue in the cases of the main proceedings, taking into account, in particular, the general and indiscriminate nature of the interference caused by the direct introduction on the suppliers' networks, of automated processing of detection, the details of which are determined by the State intelligence agencies.

3.1. The collection of data must be in compliance with the requirements of the Charter

45. A national measure requiring a supplier to allow access or collection of traffic or location data falls within the scope of Directive 2002/58, even though no specific requirement has been imposed.

46. Article 3 of Directive 2002/58 states that it “applies to the processing of personal data in connection with the provision of publicly available electronic communications services on public communication networks within the European Community".

47. As the Grand Chamber has held, this measure falls within the scope of that directive as a regulation of the activities of electronic communications service providers, where such activity necessarily involves the processing of personal data by the electronic communications service provider (Tele2/Watson judgment, Paragraph 75).

48. Article 4 of the GDPR defines processing as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available”.

49. Therefore, real-time data collection involves, for the electronic communications service provider, a form of data processing that it carries out in the course of its activities; as such, this falls under Article 15 as well as Article 3 of Directive 2002/58 and must therefore comply with the requirements of the Charter.

50. The fact that the national regulations in question pursue a purpose relating to the safeguarding of national security does not exempt those measures from compliance with the Charter, since they constitute limitations on the rights and obligations provided for by European Union law. (see Paragraph 32, Page 11). Accordingly, the substantive and procedural guarantees provided for by the Grand Chamber in its case-law must be respected in order to ensure that national variances are adequately limited to what is strictly necessary and proportionate.

3.2. Appropriate substantive and procedural guarantees must be respected

51. A requirement for real-time collection of traffic and location data constitutes a particularly serious interference with the right to privacy of the data subjects. It may, however, be justified for sufficiently serious aims commensurate with the gravity of the interference, provided that appropriate safeguards are provided to ensure that such data handling is limited to what is strictly necessary (see, by correlation, Tele2/Watson judgment, Paragraph 117). In particular, these guarantees must comply with both substantive and procedural conditions.

52. As regards the substantive conditions, limitations on the scope of the data must be imposed. In particular, the processing of data causing an interference as serious as that described above, cannot be related to persons for whom there is no evidence to legitimately suggest that they have any link with the legitimate objectives being pursued, or for which there is no objective evidence that such data could, in a specific case, make an effective contribution to the vital interests of national security (see, by correlation, Tele2/Watson, Paragraphs 105 and 119 and, in regard to Directive 2006/24, Digital Rights judgment, Paragraph 57).

53. Regarding the procedural requirements, the Court has already held, "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". (Tele2/Watson, Paragraph 120 [emphasis added by the Intervener], see also: Digital Rights judgment, Paragraph 62).

54. In this respect, the authorization to collect data in real time cannot be considered subject to conditions meeting the necessary procedural guarantees described by the Grand Chamber, when these conditions include only a single basic opinion of one independent administrative authority, which is non-binding and does not constitute a "decision".

55. The European Court of Human Rights also considers that an independent and prior authorization is a minimum guarantee to protect the right to privacy, especially in the context of secret surveillance (see, for example, the Zakharov judgment, Paragraph 233; see also ECtHR, Jan. 12 2016, Szabó v. Hungary, no 37138/14, Paragraph 77).

4. THIRD QUESTION IN CASE No. C-511/18

56. Essentially, the Court has been asked to determine whether the notification requirement to affected individuals, when such notification is no longer capable of jeopardizing investigations by the competent authorities, is essential in ensuring the right to redress, or if other procedural safeguards can effectively provide a right of recourse in the absence of such information.

57. The Intervener states that since the collection of connection data constitutes a limitation of the rights of the persons concerned under Directive 2002/58, the procedure surrounding such a collection must comply with the European Charter and in particular the right to effective remedy. Such a procedure, by its secrecy and absence of notification, also constitutes a limitation of the rights of an individual to access information on the processing of their personal data, as well as the obligations of data controllers under the GDPR. It must therefore be in conformity with the Charter.

58. **Firstly**, the notification to the persons concerned, from the moment this communication is no longer likely to compromise investigations being conducted by the competent authorities, is considered, by the Grand Chamber of the Court of Justice, to be "in fact, necessary" to enable the exercise of the rights of the individual and in particular the right to a legal remedy in the event of a violation (Tele2/Watson, Paragraph 121).

59. If the right to effective remedy requires access to the relevant information, the justification for safeguarding national security cannot preclude any communication with the person concerned.

60. By extension, if judicial protection can be adjusted to take into account legitimate considerations regarding State security, the procedural rules must nevertheless reconcile these considerations, on the one hand, and the need to guarantee compliance with procedural rights on the other. The Court ruled that "the requirements to be met by judicial review of the existence and validity of the reasons invoked by the competent national authority with regard to State security of the Member State concerned, it is necessary for a court to be entrusted with verifying whether those reasons stand in the way of precise and full disclosure of the grounds on which the decision in question is based and of the related evidence" (Grand Chamber of the Court, June 4, 2013, ZZ, C-300/11, Paragraph 60). Therefore, as the Grand Chamber of the Court has already held, " the competent national authority has the task of proving, in accordance with the national procedural rules, that State security would in fact be compromised by precise and full disclosure to the person concerned of the grounds which constitute the basis of a decision taken […]. It follows that there is no presumption that the reasons invoked by a national authority exist and are valid [and that] the national court with jurisdiction must carry out an independent examination of all the matters of law and fact relied upon by the competent national authority and it must determine, in accordance with the national procedural rules, whether State security stands in the way of such disclosure" (ZZ judgment, Paragraphs 61 and 62). Equivalent considerations apply in these cases, in order to achieve a balanced conciliation between the needs of safeguarding national security and the right to effective remedy of the persons concerned.

61. Under international law, it is the State that bears the burden of demonstrating the effectiveness of the remedy, in particular as regarding limitations on the right of redress in relation to respect for private life (ECtHR, 3rd Sect. Feb. 3, 2015, Pruteanu v. Romania, no 30181/05).

62. **Secondly**, this information is generally required by EU law for the protection of personal data, even if it may be delayed so as not to compromise the objectives of the reason for the processing of the data.

63. Article 12 of the GDPR requires data controllers to facilitate the exercise of an individual's rights regarding data. In accordance with the principle of transparency, individuals must therefore be informed, including when data is obtained from a third

party, pursuant to Article 14. This may not be delayed when such communication is likely to render impossible or seriously jeopardize the achievement of the objectives of the data processing, itself. In such cases, the communication of information must be made as soon as this communication is no longer likely to compromise the objectives of the data processing. This is the interpretation provided by the data protection authorities (under the aegis of Directive 95/46). In their Opinion 1/2006, filed February 1, 2006, the Article 29 Working Party stated that "where there is substantial risk that such notification would jeopardise the ability of the company to effectively investigate the allegation or gather the necessary evidence, notification to the incriminated individual may be delayed as long as such risk exists. This exception to the rule provided by Article 11 is intended to preserve evidence by preventing its destruction or alteration by the incriminated person. It must be applied restrictively, on a case-by-case basis, and it should take account of the wider interests at stake."

64. Finally, it would be surprising, to say the least, if the approach adopted by the European Parliament and the Council for the processing of personal data by the competent authorities for the purpose of preventing and detecting criminal offenses, investigations and prosecutions in this respect, is not equally balanced by the context of the processing of personal data by the administrative authorities for the purpose of safeguarding the fundamental interests of the nation.[14] In this respect, Article 12 of Directive 2016/680 provides "reasonable steps to provide any information referred to in Article 13 […] relating to processing to the data subject in a concise, intelligible and easily accessible form, using clear and plain language". Article 13 of that directive provides that legislative measures may be adopted and "delaying, restricting or omitting the provision of the information to the data subject", but these terms and conditions may only apply " as long as such a measure constitutes a necessary and proportionate measure in a democratic society, with due regard for the fundamental rights and the legitimate interests of the natural person concerned". It is important, in any event, that this exception be strictly interpreted and that the burden of proof of the need to derogate from the requirement to provide information rests with the authorities, so as not to violate the provisions as set forth by Article 13, Paragraphs 1 and 2.

65. **Thirdly** and finally, the information of the person concerned is considered as a guarantee of the effective recourse under international law. In the Zakharov judgment cited above, the Grand Chamber of the European Court of Human Rights reiterated that "after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers." (§234). In fact, " there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively (see Klass and Others, cited above, §

[14] Regarding the scope of this notion of the fundamental interests of the Nation and, in particular, its inclusion as part of the field of criminal law, see Footnotes 10, 11 and 12 on page 6.

57, and Weber and Saravia, cited above, § 135) or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications (see Kennedy, cited above, § 167)." (Ibid.)

66. Similarly, the Council of Europe's Commissioner for Human Rights, in a memorandum dated May 17, 2016, was in favour of a system of notification of persons under surveillance, beginning the moment the surveillance is no longer compromised by said notification (Paragraph 25 [Exhibit No. A.3]).

67. In conclusion, the requirement to notify an individual, when this notification will no longer compromise the investigations of the competent authorities, is the result of a balanced conciliation between safeguarding national security and the right to redress. Such a requirement would, moreover, be consistent with European Union law on the protection of personal data, which must be equivalent in all Member States since the entry into force of the GDPR. Finally, such a requirement would be compatible with international law.

For these reasons, the Intervener invites the Court to rule as follows:

On the first questions raised by Case Nos. C-511/18 and C-512/18

Article 15 (1) of Directive 2002/58, read in the light of the European Charter, must be interpreted as precluding national rules providing, for the purpose of ensuring national security, the widespread and indiscriminate retention of all subscriber and user connection data imposed on providers, notwithstanding the safeguards and controls that accompany the subsequent collection and use of such data, and notwithstanding the context of significant and persistent threats to national security.

On the second question raised by Case No. C-511/18

Article 15 (1) of Directive 2002/58, read in the light of the Charter, must be interpreted as precluding national rules governing the real-time collection of traffic data and the location of specific individuals which affect the rights and obligations of the providers of electronic communications services, without limiting this collection to purposes justifying the seriousness of the interference caused by such a collection, and without submitting this collection to the prior authorization of a Court or an independent administrative authority in a quasi-jurisdictional function.

On the third question raised by Case No. C-511/18

Article 15 of Directive 2002/58, read in conjunction with Articles 7, 8 and 47 of the European Charter, and read in conjunction with Article 22 of Directive 95/46, Article 79 of the GDPR and the Article 54 of Directive 2016/680, shall be interpreted as precluding national rules governing the collection by national authorities of connection data relating to one or more persons, without notifying the persons concerned as soon as the notification is no longer likely to jeopardize investigations carried out by those authorities.

HUGO ROY
[signed]

ATTORNEY AT LAW OF THE PARIS BAR

EXHIBITS

(A) 1. Conclusions of Mr. Édouard Crépey, Public Rapporteur for the Council of State, regarding the Chambers meeting of 11 July 2018 of the 10th and 9th, Case Nos 393099, 394924, 394922, 394925, 397844 and 397851, French Data Network et al (see above, Paragraph 16 Page 7).

2. Opinion 1/2006 on the application of EU data protection rules to internal mechanisms for reporting malfunctions in the areas of accounting, internal accounting controls, audits, the fight against corruption and banking and financial crimes, adopted on 1 February 2006 by the "Article 29" Data Protection Working Group (see above, Paragraph 63, Page 17).

3. Memorandum on surveillance and oversight mechanisms in the United Kingdom, May 17, 2016, of the Commissioner for Human Rights, Council of Europe (see above, Paragraph 66, Page 18).